CHECKLIST ATTACHMENT VERSION DATE:
FEBRUARY 22, 2002

ENERGY INFRASTRUCTURE VULNERABILITY SURVEY CHECKLISTS FOR [FACILITY NAME, FACILITY LOCATION] (X)

prepared by
Argonne National Laboratory
Idaho National Energy and Environmental Laboratory
Lawrence-Livermore National Laboratory
Los Alamos National Laboratory
Oak Ridge National Laboratory
Pacific Northwest National Laboratory
Sandia National Laboratory

Month Day, Year

prepared for
Office of Energy Assurance
U.S. Department of Energy

Special Information:
Specific Name:
Special Date:

(X) PREFACE

(X) Effective operation of the U.S. energy infrastructure is critical to the health and safety, national security, and economic viability of the nation. As the lead agency for the energy industry, the Department of Energy's near-term efforts include assuring the reliability and security of the energy infrastructure. At an initial step towards this end, a series of vulnerability surveys are being conducted for 25 critical energy infrastructure assets across the United States by teams of national laboratory experts. To more readily obtain information concerning specific energy infrastructure assets through interviews with the executives and staff of the organizations that own or operate these assets, non-disclosure agreements between the organizations and the national laboratories conducting the surveys. Therefore, the information contained in these vulnerability survey documents must be considered "BUSINESS SENSITIVE" and is not to be distributed freely.

(X) Survey Team

(X) • Name, Affiliation/Laboratory, Responsibility

(X) • Name, Affiliation/Laboratory, Responsibility

(X) • Name, Affiliation/Laboratory, Responsibility

(X) Report Preparation Team

(X) • Name, Affiliation/Laboratory, Responsibility

(X) • Name, Affiliation/Laboratory, Responsibility

TABLE OF CONTENTS (X)

(This page contains … .)

ENERGY INFRASTRUCTURE VULNERABILITY SURVEY CHECKLISTS FOR [FACILITY NAME, FACILITY LOCATION] (X)

INTRODUCTION (X)

(X) The attachments contain checklists to be used in the survey. The following general points can be made about the checklists.

(X)
- The completed checklists will become part of the official documentation of the survey. Teams should transcribe any handwritten notes taken on the checklists and submit them with the report (*Energy Infrastructure Vulnerability Survey for* [FACILITY NAME, FACILITY LOCATION]).

(X)
- If absolutely needed, it is acceptable to put notes and comments on separate sheets or in separate computer files along with a reference note in the checklist itself. (I.e., if it is not possible to fit the material into the space provided in the checklist, put a numbered note in the checklist form that references attached sheets/files.)

(X)
- Each entry in the checklist should be accompanied by an indication of where the information came from (e.g., "Interview with Security Director" or "From company policy manual").

(X)
- If a checklist or a question in a checklist does not apply, the information is not available, or the area was not included in the survey, indicate so with "Not Applicable," "Not Available," or "Not Included in Survey," as appropriate.

(X)
- In the case of checklists that apply to individual critical assets that partially make up the entire facility being surveyed, duplicate the checklist and insert the correct asset name [ASSET] in the header. Keep the original checklist number (e.g., CHECKLIST G.3) to maintain the correct link to the portion of the report template into which that information feeds.

ATTACHMENT A: FACILITY IDENTIFICATION (X)

(X) This checklist provides information that will be used to generate a general description of the facility.

CHECKLIST A.1 FACILITY IDENTIFICATION (X)

XXXXXXXXXXXX	
Date: [MONTH XX, 2002] Facility: [FACILITY]	
	INFORMATION/COMMENTS
(a) Contact Information	
Full Facility Name	
Facility Address	
Point of Contact #1	
Title	
Phone	
FAX	
E-mail	
Point of Contact #2	
Title	
Phone	
FAX	
E-mail	
Point of Contact #3	
Title	
Phone	
FAX	
E-mail	
Point of Contact #4	
Title	
Phone	
FAX	
E-mail	
Point of Contact #5	
Title	
Phone	
FAX	
E-mail	
(b) General Descriptive Information	
Facility type (e.g., power plant, refinery)	
Principal function(s) of the facility (e.g., electricity	

CHECKLIST A.1 FACILITY IDENTIFICATION (X)

XXXXXXXXXXXXX	
Date: [MONTH XX, 2002] Facility: [FACILITY]	
	INFORMATION/COMMENTS
production, crude oil transport)	
Facility size (e.g., capacity – megawatts, throughput – barrels per day)	
Facility location (e.g., distance from nearest city, routes for pipelines)	
Facility layout (Describe physical layout and/or provide a map/schematic of layout if available.)	
Characteristics of the surrounding area (e.g., densely populated, rural)	
Number of employees at the facility	

ATTACHMENT B: CRITICAL ASSET IDENTIFICATION (X)

(X) These checklists identify critical assets at the facility. A critical asset is a component or element of the facility (e.g., a piece of equipment, a building, a connection to a supporting utility), which, if damaged or destroyed, would either:

- Force the facility to operate at a much reduced level, or
- Disable the facility completely.

(X) Complete one full section of Checklist B.1 for each identified critical asset.

In the case of checklists that apply to individual critical assets that partially make up the entire facility [FACILITY] being surveyed, duplicate the checklist and insert the correct asset name [ASSET]. Keep the original checklist number (e.g., CHECKLIST B.1) to maintain the correct link to the portion of the report template into which that information feeds.

CHECKLIST B.1 CRITICAL ASSET IDENTIFICATION (X)

XXXXXXXXXXXXX	
Date: [MONTH XX, 2002] Facility: [FACILITY]	
This checklist applies to [ASSET]	
(a) Asset Information	
Asset name	
Location of asset at facility	
Function of asset at facility (i.e., what role does the asset play at the facility?)	
(b) Asset Damage Impact	
Impact of the loss of the asset (e.g., would cause shutdown, would allow only limited partial operation, interdependency with other assets exists)	
Redundancy for the asset (e.g., available backup facilities, equipment, or capabilities)	
Repair and replacement issues for the asset (e.g., difficult to repair, long lead time for replacement, expensive to repair or replace)	

ATTACHMENT C: THREAT APPLICABILITY (X)

(X) This checklist considers the types of threats that are applicable to this facility and its critical assets. The probability of effectiveness (P_E) is used to summarize the overall nature of the existing security system effectiveness against applicable threats. The criteria for assigning P_E values are:

(X)

- **P_E = Low:** The facility/asset security system would have less than a 50% probability of defeating this type of attack by the specified type of adversary,

(X)

- **P_E = Moderate:** The facility/asset security system would have a 50% to 80% probability of defeating this type of attack by the specified type of adversary, and

(X)

- **P_E = High:** The facility/asset security system would have greater than an 80% probability of defeating this type of attack by the specified type of adversary.

(X) The two types of adversaries specified are:

(X)

- **Individual (I):** An individual adversary, and

(X)

- **Team (T):** An adversary team of up to five members.

In the case of checklists that apply to individual critical assets that partially make up the entire facility being surveyed, duplicate the checklist and insert the correct asset name [ASSET]. Keep the original checklist number (e.g., CHECKLIST C.1) to maintain the correct link to the portion of the report template into which that information feeds.

CHECKLIST C.1 THREAT APPLICABILITY (X)

XXXXXXXXXXXXX				
Date: [MONTH XX, 2002] Facility: [FACILITY]				
This checklist applies to [the entire facility/ASSET]				
Instructions: For each threat, in the appropriate **P_E** column enter an "**I**" for an individual adversary and "**T**" for an adversary team of up to five members. In the comments section, include an identification of likely targets at the facility/asset for an attack using that method, the most likely scenarios of how such an attack would be mounted, and a list of events that the facility has experienced with the method.				
	P_E			**COMMENTS**
	High	**Mod**	**Low**	
Define and describe the adversary objective against which the **P_E** ratings are defined.				
Method of Attack	**P_E**			
	High	**Mod**	**Low**	
(a) Explosives and Incendiary Devices				
Car/truck devices				
Other vehicle-delivered devices (e.g., boat, rail)				
Mail-delivered devices				
Individual-delivered (e.g., suicide) devices				
Standoff weapons (e.g., artillery, rockets)				
Airplane impact				
Other explosive or incendiary devices (specify)				
(b) Sabotage				
Equipment				
Operations				
(c) Assault				
Individual attacker – lightly or heavily armed				
Team of attackers – lightly or heavily armed				
Other				
(d) Theft/Alteration/ Release of Information, Materials, or Equipment				
Operations information,				

CHECKLIST C.1 THREAT APPLICABILITY (X)

XXXXXXXXXXXXX

Date: [MONTH XX, 2002] Facility: [FACILITY]

This checklist applies to [the entire facility/ASSET]

Instructions: For each threat, in the appropriate **P_E** column enter an "**I**" for an individual adversary and "**T**" for an adversary team of up to five members. In the comments section, include an identification of likely targets at the facility/asset for an attack using that method, the most likely scenarios of how such an attack would be mounted, and a list of events that the facility has experienced with the method.

	P_E			**COMMENTS**
	High	**Mod**	**Low**	
materials, or equipment				
Business/proprietary information				
Hazardous materials or weapons material				
(e) Contamination				**NOTE: Only a brief identification of contamination threats is to be included in this survey.**
Chemical agents				
Biological agents				
Radioactive material				
Other				
(f) Cyber Attack				**NOTE: Only a brief identification of cyber threats is to be included in this survey.**
(g) Other Threats				

ATTACHMENT D: SECURITY PROGRAM MANAGEMENT (X)

(X) The focus of this portion of the survey is on the security organization at the facility and the programs and plans that are in place.

CHECKLIST D.1 SECURITY PROGRAM MANAGEMENT (X)

XXXXXXXXXXXX	
Date: [MONTH XX, 2002]	Facility: [FACILITY]
	COMMENTS
(a) Security Organization	
Is there a senior level security working group with representatives from each major office or department to establish security policies (including physical security, operations security, and infrastructure interdependencies security) and integrate them across all elements of the organization? • If there is a senior level security working group, describe the membership, the lines of communication, and any scheduled periodic meetings to resolve security issues. • If there is not such a group, how are security policies established?	
Is there a security office that is responsible for implementing security policies and procedures (including physical security, operations security, and infrastructure interdependencies security)? • If there is a security office, where does it report in the organization, how many people are in the office, and are resources adequate? Also describe any training received. • If there is not such an office, how are security policies implemented?	

CHECKLIST D.1 SECURITY PROGRAM MANAGEMENT (X)

XXXXXXXXXXXX	
Date: [MONTH XX, 2002]	Facility: [FACILITY]
	COMMENTS
(b) Security Plans and Policies	
Is there a mission statement describing the physical security, operations security, and infrastructure security programs?	
Is there a formal security plan and statement of security policies? If there is, describe it including how it is communicated to employees.	
Is there a formal threat definition and assessment statement? If there is, describe it including how it is communicated to employees.	
(c) Security Resources	
Are the resources (budget and staffing) applied to security (including physical security, operations security, and infrastructure interdependencies security) considered adequate?	
Do security personnel feel that they have adequate training to accomplish their functions?	
(d) Senior Management Security	
Is there an executive protection program for senior executives/managers? If there is such a program, describe it.	
Is public information on senior executives/managers controlled? If it is, describe how it is controlled.	
(e) Security Audits	
Is there a regular security assessment or audit? If there is, describe how it is done, by whom, and how frequently.	

CHECKLIST D.1 SECURITY PROGRAM MANAGEMENT (X)

XXXXXXXXXXXX	
Date: [MONTH XX, 2002]	Facility: [FACILITY]
	COMMENTS
Has the most recent audit indicated any weaknesses? Summarize the results of the audit, particularly any weaknesses identified.	
Have any corrective measures been implemented recently? Describe them.	
(f) Handling of Sensitive Information	
How is sensitive information identified and marked?	
Who has access to sensitive security information?	
How is sensitive information protected, stored, accessed, transmitted, and destroyed?	
How do senior executives/managers protect sensitive security information?	

ATTACHMENT E: PHYSICAL SECURITY SURVEY (X)

(X) The objective of the physical security portion of the survey is to identify measures that protect the entire facility and/or each critical asset of the facility, and to determine the effectiveness of the protection. This attachment contains checklists that are used to conduct the physical security portion of the survey. Checklist D.1 is used to identify physical security measures that may be present to protect the entire facility or a critical asset at the facility. The remaining checklists are used to specifically evaluate the individual elements of the physical security system that are present. The conclusion of whether a particular element provides adequate protection is to be reported as part of the findings in the body of the survey results report (Section 4). A "set" of checklists should be completed for the facility as a whole and for each of the critical assets within the facility.

(X) Note that the infrastructure interdependencies portion of the survey will identify infrastructures that support the facility and/or its critical assets (e.g., electric power, water, and telecommunications). A physical security review of these vital infrastructures should also be conducted.

(X) The checklists that are included here are:

E.1 Identification of Physical Security Measures,
E.2 Threat Detection and Evaluation Capabilities,
E.3 Perimeter Barriers,
E.4 Building Barriers,
E.5 Intrusion Detection,
E.6 Access Control,
E.7 Security Force, and
E.8 Summary of Physical Security Element Effectiveness.

In the case of checklists that apply to individual critical assets that partially make up the entire facility being surveyed, duplicate the checklist and insert the correct asset name [ASSET]. Keep the original checklist number (e.g., CHECKLIST E.3) to maintain the correct link to the portion of the report template into which that information feeds.

CHECKLIST E.1 IDENTIFICATION OF PHYSICAL SECURITY SYSTEMS (X)

XXXXXXXXXXXXX

Date: [MONTH XX, 2002] Facility: [FACILITY]

This checklist applies to [the entire facility/ASSET]

Instructions: Checklist E.1 identifies the physical security elements that may be used to protect the entire facility and/or a critical asset. Identify which elements are present for the facility or the critical asset listed above. Once physical security elements are identified, they can be reviewed by using the applicable checklists E.2 – E.6. At the completion of the reviews, the effectiveness of the elements is to be documented in the body of the survey report.

Physical Security System Element	Element Present		COMMENTS
	Yes	No	
Perimeter Barriers			
Building Barriers			
Intrusion Detection			
Access Controls			
Security Force			

CHECKLIST E.2 THREAT DETECTION AND EVALUATION CAPABILITIES (X)

XXXXXXXXXXXX	
Date: [MONTH XX, 2002] Facility: [FACILITY]	
This checklist applies to the entire facility	
	COMMENTS
(a) Threat Analysis Working Group	
Is the organization a member of a local threat analysis working group? Describe the group	
If the organization is a member of such a group, list the organizations that participate in the working group (e.g., local, county, state, and federal agencies, the military).	
Are there other industry partners participating in the working group? Describe them.	
Are active efforts being made to recruit other meaningful participants into the working group? Describe the efforts.	
Do the participants in the working group have management support, requirements, and funding to participate? Describe the situation.	
Are the members of the working group willing participants and do they work against bureaucratic obstacles that may prevent the success of the group? Describe the situation.	
Do the members of the working group have the authority to share information with other members of the group? Describe the situation.	
Have the members of the working group been given appropriate U.S. government clearances to share in threat information? Describe the situation.	
Do the members of the working group have access to the National Infrastructure Protection Center (NIPC), Analytical Services, Inc.,	

CHECKLIST E.2 THREAT DETECTION AND EVALUATION CAPABILITIES (X)

XXXXXXXXXXXX	
Date: [MONTH XX, 2002]	Facility: [FACILITY]
This checklist applies to the entire facility	
	COMMENTS
(ANSER), FBI-sponsored InfraGuard, Carnegie Mellon University's CERT®, and other information system security warning notices? List the threat information systems they use.	
Indicate the frequency and regularity of the working group meetings.	
Do the members of the working group have processes in place to obtain real-time information from the field (e.g., on-duty offices, civilian neighborhood watch programs, local businesses, other working groups in the area)? Describe these processes.	
Do members of the working group have the ability to initiate information-gathering requests back into the field environment? Describe the capability.	
Are the threat statements developed by the working group specific to the organization or the industry, versus general nationwide warnings? Describe the process for gathering these statements.	
Do some members of the working group conduct scheduled meetings with the public to discuss concerns and observations? Describe these interactions.	
Do the members of the working group know what the critical assets of the organization are? Describe the extent of their knowledge.	
Do the members of the working group understand industry interdependencies and work with	

CHECKLIST E.2 THREAT DETECTION AND EVALUATION CAPABILITIES (X)

XXXXXXXXXXXXX	
Date: [MONTH XX, 2002] Facility: [FACILITY]	
This checklist applies to the entire facility	
	COMMENTS
other industry members to address these potential concerns? Describe the extent of these interactions.	
What are the roles and responsibilities of the working group members during response and recovery activities?	
Is an annual industry threat impact study written to document the threat analysis working group findings? Describe the scope of the document.	
(b) Organization's Response to Threat Updates	
Does senior management support and/or participate in the threat analysis working group? Describe the extent of the support/participation.	
Does the organization receive as-needed threat briefings from local, state, and federal agencies? Describe the nature and extent of the briefings.	
Does the organization have the ability to distribute organization-specific threat warnings in real time? Describe the process.	
Does the organization have the ability to augment security programs based on threat updates? Describe the process.	
Does the organization conduct historical trending analysis for security events (both planned and actual) and implement security activates to mitigate them? Describe the analysis.	
Does the organization create possible threat scenarios based on input from the threat analysis	

CHECKLIST E.2 THREAT DETECTION AND EVALUATION CAPABILITIES (X)

XXXXXXXXXXXXX	
Date: [MONTH XX, 2002]	Facility: [FACILITY]
This checklist applies to the entire facility	
	COMMENTS
working group and conduct related security exercises? Describe the exercises.	

CHECKLIST E.3 PERIMETER BARRIERS – FENCES, GATES (X)

XXXXXXXXXXXXX	
Date: [MONTH XX, 2002] Facility: [FACILITY]	
This checklist applies to [the entire facility/ASSET]	
	COMMENTS
(a) Fences	
Characterize fence construction and rate the level of security it provides as low, moderate to high, or other (specify). • Low: no fence or only an 8-foot chain-link fence. • Moderate to high: 8-foot chain-link fence with outriggers, 8 to 12-foot chain-link fence with outriggers, or over 12-foot chain-link fence with outriggers.	
Characterize fence signage as no signs, posted “No Trespassing,” or other (specify).	
Characterize the fence alarm system as no alarms, fence sensors (taut wire, vibration, strain, electric field, or multiple sensors), or other (specify).	
Fence area: • Is the fence within 2 inches of firm hard ground? • Is the fence line clear of vegetation, trash, equipment, and other objects that could impede observation? • Is the area free of objects that would aid in traversing the fence? • Is physical protection installed for all points where utilities (e.g., electric power lines, natural gas pipelines, telecommunication lines, water supply, storm sewers, drainage swells) intersect the fence perimeter?	

CHECKLIST E.3 PERIMETER BARRIERS – FENCES, GATES (X)

XXXXXXXXXXXXX	
Date: [MONTH XX, 2002] Facility: [FACILITY]	
This checklist applies to [the entire facility/ASSET]	
	COMMENTS
How is the fence protected from vehicles (aircraft cable, concrete barriers or median, guard rails, steel posts, a ditch, crash I-beams, train barrier, or other [specify])?	
Fence illumination: • Is there security lighting for the fences? Describe the security lighting system. • Do alarms or infrared detectors trigger the lighting? Describe the triggering process.	
(b) Gates	
Characterize the gates as no gate closure, vehicle bar, chain-link fence, or other (specify).	
Characterize the gate locks as no lock, lock not used, gate unlocked, gate attended by personnel when unlocked, ID actuated lock, padlock, or other (specify).	
How is access to gate keys controlled?	
Gate lighting: • Describe the security lighting for the gates. • Do alarms or infrared detectors trigger the lighting? Describe the triggering process.	
(c) Vehicle Barriers	
Characterize vehicle barriers as none, a vehicle bar, blocked by vehicle when gate open, hydraulic wedge, or other (specify).	

CHECKLIST E.4 BUILDING BARRIERS – WALLS, ROOF/CEILING, WINDOWS, DOORS (X)

XXXXXXXXXXXXX	
Date: [MONTH XX, 2002] Facility: [FACILITY]	
This checklist applies to [the entire facility/ASSET]	
	COMMENTS
(a) Walls	
Characterize wall construction and rate the level of security wall provide as low, moderate, or high. • Low: chain-link mesh, 16-gauge metal, wood studs and dry wall, wood studs and plywood, or other (specify). • Moderate: clay block, 8-inch hollow block, 8-inch filled block, or other (specify). • High: 8-inch filled rebar block, 12-inch filled rebar block, 2-inch precast concrete tees, 4-inch reinforced concrete, 8-inch reinforced concrete, 12-inch reinforced concrete, 24-inch reinforced concrete, or other (specify).	
Do the walls extend from the floor to the structural ceiling?	
(b) Roof/Ceiling	
Characterize the roof material and rate the level of security it provides as low, moderate, or high. • Low: 20-gauge metal with insulation, ½-inch wood, or other (specify). • Moderate: 20-gauge metal built-up roof, concrete built-up roof with T-beams, or other (specify). • High: 5-½-inch concrete roof, 8-inch concrete roof, 3-foot earth cover, 3-foot soil/cement/earth cover, or other (specify).	
Does the interior drop ceiling extend beyond the structural walls?	

CHECKLIST E.4 BUILDING BARRIERS – WALLS, ROOF/CEILING, WINDOWS, DOORS (X)

XXXXXXXXXXXXX	
Date: [MONTH XX, 2002]	Facility: [FACILITY]
This checklist applies to [the entire facility/ASSET]	
	COMMENTS
(c) Windows	
Characterize the window materials and rate the level of security they provide as low or moderate. • Low: standard windows or other (specify). • Moderate: 9-gauge expanded mesh, ½-inch diameter x 1-¼-inch quarry screen, ½-inch diameter bars with 6-inch spacing, $^{3}/_{16}$-inch x 2-½-inch grating, or other (specify).	
Characterize the window alarms (for windows that would be accessible by foot or ladder) as none, vibration sensor, glass breakage sensor, conducting tape, grid mesh, multiple sensors, or other (specify).	
(d) Doors	
Characterize door materials and rate the level of security they provide as low, moderate, or high. • Low: wood, 9-gauge wire mesh, hollow-core metal, no lock/hinge, or other (specify). • Moderate: hollow-core metal, tempered-glass panel, security-glass panel, half-height turnstile, or other (specify). • High security: ½-inch steel plate, turnstile – aluminum, Class V or VI vault, or other (specify).	

CHECKLIST E.4 BUILDING BARRIERS – WALLS, ROOF/CEILING, WINDOWS, DOORS (X)

XXXXXXXXXXXX	
Date: [MONTH XX, 2002]	Facility: [FACILITY]
This checklist applies to [the entire facility/ASSET]	
	COMMENTS
Characterize the door locks and rate the level of security they provide as low, moderate, or high. • Low: none, lock not used, or other (specify). • Moderate: door unlocked, attended by personnel when unlocked, ID actuated lock, padlock, keyed cylinder lock, combination lock, mechanically coded lock, or other (specify). • High: electronically coded lock, two-person rule lock system, lock inaccessible from the door exterior, or other (specify).	
How is access to the keys for the door locks controlled?	
Door Alarms: • Is door position monitored? • Indicate the type of door penetration sensor (vibration, glass breakage, conducting tape, grid mesh, or other [specify]).	

CHECKLIST E.5: INTRUSION DETECTION (X)

XXXXXXXXXXXX	
Date: [MONTH XX, 2002] Facility: [FACILITY]	
This checklist applies to [the entire facility/ASSET]	
	COMMENTS
(a) Intrusion Sensors	
Characterize the exterior intrusion sensors as seismic buried cable, electric field, infrared, microwave, video motion, or other (specify).	
Characterize the interior intrusion sensors as sonic, capacitance, video motion, infrared, ultrasonic, microwave, or other (specify).	
(b) Intrusion Alarm Deployment	
Characterize intrusions alarm deployment in terms such as: • continuously monitored, • positioned to prevent gaps in coverage, • detection zone kept clear of obstructions (e.g., dips, equipment, snow, ice, grass, debris), • tamper and system problem indicators provided, • compensatory measures employed when alarms are not operating, • backup power provided, and • other (specify).	
(c) Intrusion Alarm Assessment	
Characterize the assessment of intrusion alarms as not assessed, closed circuit TV, automatic deployment of protective force, or other (specify).	
(d) Intrusion Alarm Maintenance	
Characterize intrusion alarm maintenance in terms such as: • routine preventive maintenance performed regularly, • functional testing performed regularly,	

CHECKLIST E.5: INTRUSION DETECTION (X)

XXXXXXXXXXXXX	
Date: [MONTH XX, 2002]	Facility: [FACILITY]
This checklist applies to [the entire facility/ASSET]	
	COMMENTS
• maintenance personnel have appropriate clearances, and • other (specify).	

CHECKLIST E.6 ACCESS CONTROL (X)

XXXXXXXXXXXX	
Date: [MONTH XX, 2002] Facility: [FACILITY]	
This checklist applies to [the entire facility/ASSET]	
Note: Different access points to the facility and/or to critical assets may have different access controls. The comments should clearly distinguish whether the evaluation applies to all access points or to specific access points.	
	COMMENTS
(a) Personnel Access	
Characterize access point control as unmanned, unarmed guard, armed guard, or other (specify).	
Characterize the identification check process as none in place, casual recognition, credential check (e.g., drivers license, passport, state ID), picture badge, PIN, exchange badge, retinal scan, hand geometry, speech pattern, signature dynamics, fingerprint, or other (specify).	
Characterize the organization's badging policy in terms such as no badging policy, visitor badges required, badge issuance and control procedures in place (describe), and badges show permission to access specific areas (describe).	
(b) Vehicle Access	
Characterize vehicle access point controls as unmanned, unarmed guard, armed guard, or other (specify).	
Characterize the vehicle access identification process as none in place, vehicle stickers, vehicle stickers with personnel identification, automated system (describe), or other (specify).	
(c) Contraband Detection	
Characterize explosives detection capabilities as none in place, animal olfaction, vapor collection, thermal neutron, or other (specify).	

CHECKLIST E.6 ACCESS CONTROL (X)

XXXXXXXXXXXXX	
Date: [MONTH XX, 2002] Facility: [FACILITY]	
This checklist applies to [the entire facility/ASSET]	
Note: Different access points to the facility and/or to critical assets may have different access controls. The comments should clearly distinguish whether the evaluation applies to all access points or to specific access points.	
	COMMENTS
Characterize metal detection capabilities (handheld or portal) as none, ferrous metals, or lead materials.	
Characterize item and vehicle search procedures as none, cursory, or detailed	
(d) Access Point Illumination	
Access Point Illumination: • Is there security lighting for the access points? Describe the security lighting system. • Do alarms or infrared detectors trigger the lighting? Describe the triggering process.	

CHECKLIST E.7 SECURITY FORCE (X)

XXXXXXXXXXXXX	
Date: [MONTH XX, 2002]	Facility: [FACILITY]
This checklist applies to [the entire facility/ASSET]	
	COMMENTS
(a) Protective Force	
Specify the size of the protective force in terms or total number and the number on duty during working hours, non-working hours, and weekends/holidays.	
Specify the equipment available to the protective force such as uniforms; vehicles (specify number); weapons (describe), chemical, biological, radiological gear (describe); communications devices (describe); and other equipment (describe).	
Describe the training of the protective force. Specifically, describe the initial training, any continuing training (e.g., on-the-job), and drills and exercises.	
Describe the organization of the protective force. Specifically, describe the command structure, their mission as defined, any established policies and procedures, and established emergency response plans.	
Are there provisions for a back-up force (e.g., recalling off-duty personnel)? Describe the provisions in place.	
Protective Force Command Center: • Is there a protective force command and control center? Describe it. • Is there a backup center? Describe it.	
Does the protective force have arrest authority? Describe that authority.	
Are protective force operations	

CHECKLIST E.7 SECURITY FORCE (X)

XXXXXXXXXXXX	
Date: [MONTH XX, 2002]	Facility: [FACILITY]
This checklist applies to [the entire facility/ASSET]	
	COMMENTS
disguised to prevent intelligence about the facility from being inadvertently released? Describe how this is done.	
Describe protective force procedures for responding to alarms.	
Does the protective force provide security escort for visitors? Describe the nature of the escort.	
(b) Local Law Enforcement Agencies	
Describe the interaction of the protective force with local law enforcement agencies in terms of memoranda of agreement or other agreements in place (describe), protection responsibilities defined (describe), communication procedures developed (describe), and participation in drills and exercises.	
What is the approximate response time for local law enforcement personnel?	

CHECKLIST E.8 SUMMARY OF PHYSICAL SECURITY ELEMENT EFFECTIVNESS (X)

XXXXXXXXXXXXX

Date: [MONTH XX, 2002] Facility: [FACILITY]

This checklist applies to [the entire facility/ASSET]

Instructions: For each element of the physical security system, in the appropriate probability of security element effectiveness (**P_E**) column enter an "**I**" for an individual adversary and "**T**" for an adversary team of up to five members. The scale is:

- **P_E = Low** -------- The facility/asset security system element would have less than a 50% probability of defeating an attack by the specified type of adversary,
- **P_E = Moderate** - The facility/asset security system element would have a 50% to 80% probability of defeating an attack by the specified type of adversary, and
- **P_E = High** ------- The facility/asset security system element would have greater than an 80% probability of defeating an attack by the specified type of adversary.

In the comments section, provide a brief justification for the assigned **P_E** ratings.

Basis Adversary Objective

Define and describe the adversary objective against which the **P_E** ratings are defined.	

	P_E			
	High	**Mod**	**Low**	**COMMENTS**
Physical Security System Element				
Threat Detection and Evaluation Capabilities				
Perimeter Barriers				
Building Barriers				
Intrusion Detection				
Access Control				
Security Force				

ATTACHMENT F: OPERATIONS SECURITY SURVEY (X)

(X) The objective of the operations security (OPSEC) portion of the survey is to identify operational procedures and measures that protect the facility including each critical asset of the facility, and to determine the effectiveness of that protection. The conclusion of whether a measure provides adequate protection is to be reported as part of the findings in the body of the survey results report (Section 5).

(X) Note that the infrastructure interdependencies portion of the survey will identify infrastructures that support the facility and/or its critical assets (e.g., electric power, water, and telecommunications). An OPSEC review of these vital infrastructures should also be conducted.

(X) This attachment contains checklists that are used to conduct the OPSEC portion of the survey. The checklists that are included here are:

F.1 Human Resources Security Procedures,
F.2 Facility Engineering,
F.3 Facility Operations,
F.4 Administrative Support Organizations,
F.5 Telecommunications and Information Technologies,
F.6 Publicly Released Information, and
F.7 Trash and Waste Handling.

Normally, OPSEC is a corporate-wide function. Therefore, the OPSEC checklists generally will apply to the facility as a whole and will not need to be duplicated for individual critical assets.

CHECKLIST F.1 HUMAN RESOURCES SECURITY PROCEDURES (X)

XXXXXXXXXXXXX	
Date: [MONTH XX, 2002]	Facility: [FACILITY]
	COMMENTS
(a) Responsibilities	
What internal offices or departments are responsible for dealing with security-related personnel issues?	
(b) Background Checks	
What types of background checks are conducted on employees?	
How extensive are the background checks and do they vary with the sensitivity of the position?	
(c) Insider Threats	
What current conditions in the organization might create a threat from insiders (e.g., low morale, lay-offs, labor disputes)?	
What are the security procedures for handling disgruntled or at-risk employees?	
What are the security procedures for handling employee termination?	
How many employees have been terminated in the last year?	
(d) Disciplinary Procedures	
What are the policies and procedures for handling incidents of security concern?	
What are the policies and procedures for other disciplinary actions?	
(e) Security Training	
Does the organization's initial and periodic security awareness training program include sections on: security contacts, critical assets, threats, sensitive information that needs to be protected, reporting suspicious activities, and employee responsibility?	

CHECKLIST F.2 FACILITY ENGINEERING (X)

XXXXXXXXXXXXX	
Date: [MONTH XX, 2002] Facility: [FACILITY]	
This section covers security issues related to the engineering information related to the facility. Included are such things as the facility design, configuration, and layout; utility service systems; and building floor plans.	
	COMMENTS
(a) Responsibilities	
What internal offices or departments are responsible for facility engineering?	
(b) Facility Engineering Information	
What facility engineering information (e.g., engineering drawings, site maps, utility service lines, floor plans, entry paths into the facility) is considered sensitive?	
What offices or departments have control of this information?	
What other offices or departments are allowed access to this information?	
What external organizations (e.g., fire departments, environmental agencies) have been given access to this information?	
Is any of the facility engineering information publicly available?	
How is sensitive facility engineering information protected?	
What facility engineering information can be accessed via the computer system or network?	
How is the information disposed of when it is no longer needed?	
(c) Public Access to Facility	
Where are tours allowed within the facility? Describe what portions of the facility are open and who is allowed to tour.	
What portion of the facility is open to the public or special interest groups?	

CHECKLIST F.2 FACILITY ENGINEERING (X)

XXXXXXXXXXXXX	
Date: [MONTH XX, 2002] Facility: [FACILITY]	
This section covers security issues related to the engineering information related to the facility. Included are such things as the facility design, configuration, and layout; utility service systems; and building floor plans.	
	COMMENTS
What periodic meetings are held within the facility where outsiders are allowed inside the facility?	

CHECKLIST F.3 FACILITY OPERATIONS (X)

XXXXXXXXXXXX	
Date: [MONTH XX, 2002]	Facility: [FACILITY]
	COMMENTS
(a) Responsibilities	
What internal offices or departments are responsible for facility operations?	
(b) Facility Operations Control	
Is the operation of the facility controlled from a central point (or several central points)? Describe.	
Is there an automated process control system, energy management system, or supervisory control and data acquisition (SCADA) system? Is it isolated or is remote access possible?	
What facility operations control and information are on the computer systems? How is it protected? What other internal organizations have access to operations control capabilities and information?	
Can sensitive operations information be gathered through the telecommunications system (e.g., microwave, cell phones, radio, pagers, voicemail, teleconferencing)?	
Is access to the control point(s) limited to operations personnel? If not, who else has access (e.g., maintenance, janitors, vendors) and how is that access controlled?	
(c) Facility Construction, Repair, and Maintenance	
Are construction, repair, and maintenance at the facility done by employees, contractors, or both? If contractors are used, describe procedures for screening and monitoring contractor personnel.	

CHECKLIST F.3 FACILITY OPERATIONS (X)

XXXXXXXXXXXX	
Date: [MONTH XX, 2002]	Facility: [FACILITY]
	COMMENTS
Is cleaning and building maintenance (e.g., janitorial service) at the facility done by employees, contractors, or both? If contractors are used, describe procedures for screening and monitoring contractor personnel.	

CHECKLIST F.4 ADMINISTRATIVE SUPPORT ORGANIZATIONS (X)

XXXXXXXXXXXX	
Date: [MONTH XX, 2002]	Facility: [FACILITY]
	COMMENTS
(a) Procurement	**Purchasing and procurement activities include generating need (e.g., requisitions or RFPs), selecting suppliers, documenting purchases, providing delivery of items or services, and payments.**
What internal offices or departments are responsible for reviewing procurement activities from a security perspective?	
What is the security review process for RFPs, contracts, and other procurement documents?	
How is the procurement information protected before release? Include documents, files, copiers, facsimiles, and computer files?	
What security-sensitive information is uniquely marked, both on paper and electronically? Describe how.	
How is security-sensitive procurement information destroyed?	
(b) Legal	
What internal offices or departments are responsible for reviewing legal department activities from a security perspective?	
How are legal documents (e.g., patents, environmental impact statements, safety reports, Securities and Exchange Commission filings, Federal Energy Regulatory Commission filings) reviewed for security implications?	
How are these documents protected?	
How are these documents destroyed when no longer needed?	

CHECKLIST F.4 ADMINISTRATIVE SUPPORT ORGANIZATIONS (X)

XXXXXXXXXXXX	
Date: [MONTH XX, 2002]	Facility: [FACILITY]
	COMMENTS
(c) Budget and Finance	
What internal offices or departments are responsible for reviewing budget and finance activities from a security perspective?	
How are budget and finance documents reviewed for security implications?	
How are these documents protected?	
How are these documents destroyed when no longer needed?	
(d) Marketing	
What internal offices or departments are responsible for reviewing marketing activities from a security perspective?	
How are marketing materials reviewed for security implications?	
How are these documents protected?	
How are these documents destroyed when no longer needed?	
(e) Internal Information	
What are the policies and procedures for handling “Internal Use Documents” (e.g., memos, notes, newsletters)?	
How are these documents protected?	
How are these documents destroyed when no longer needed?	

CHECKLIST F.5 TELECOMMUNICATIONS AND INFORMATION TECHNOLOGY (X)

XXXXXXXXXXXX	
Date: [MONTH XX, 2002] Facility: [FACILITY]	
This checklist covers telecommunications and information technologies. Note that this part of the operations security survey must coordinated with the portions of the interdependencies survey that address the telecommunications and computer equipment.	
	COMMENTS
(a) Telecommunications	
What are the policies and procedures for communications security?	
What particular equipment carries sensitive traffic? Is this equipment restricted to selected users?	
What training is provided concerning security issues while using telecommunications equipment?	
What level of awareness is there concerning telecommunications equipment being operated in reverse as eavesdropping equipment?	
Is voicemail protected by passwords? Have users changed the vendor-supplied passwords? Is there a master password?	
How are FAX machines protected (e.g., logging, stored information, computer connectivity)?	
Is encryption used on any telecommunications circuits?	
Describe all connections to external radio nets, including paging nets?	
(b) Information Technology	
What are the policies and procedures for computing and information technology security?	
What computer architecture information is available to outsiders?	
What encryption is used for internal files and/or information transmission?	

CHECKLIST F.5 TELECOMMUNICATIONS AND INFORMATION TECHNOLOGY (X)

XXXXXXXXXXXX	
Date: [MONTH XX, 2002] Facility: [FACILITY]	
This checklist covers telecommunications and information technologies. Note that this part of the operations security survey must coordinated with the portions of the interdependencies survey that address the telecommunications and computer equipment.	
	COMMENTS
Are system administrators trained to recognize “social engineering attacks” designed to obtain passwords and other security information?	
Describe how e-mail is monitored?	

CHECKLIST F.6 PUBLICLY RELEASED INFORMATION (X)

XXXXXXXXXXXX	
Date: [MONTH XX, 2002]	Facility: [FACILITY]
This checklist covers information that is released to the public via corporate communications, press releases, the Internet, and other means.	
	COMMENTS
(a) Responsibilities	
What internal offices or departments are responsible for reviewing information (from a security perspective) that is to be released to the public?	
(b) General Procedures	
What is the process used to review information before release?	
How is the information protected before release? Include documents, files, copiers, facsimiles, and computer files.	
(c) Report Release	
Who is responsible for reviewing reports released by the organization?	
(d) Press Contacts	
Who is officially designated to interact with the press?	
How are they trained (including training on security issues)? Who trains them?	
(e) Briefings and Presentations	
Describe how briefings and presentations to be given by employees of the organization are reviewed for security issues?	
(f) Public Testimony	
Describe how public testimony that is to be given by employees of the organization is reviewed for security issues?	
(g) Internet Information	
Describe the policy for the review of information posted on the organization's Internet site for security issues?	

CHECKLIST F.6 PUBLICLY RELEASED INFORMATION (X)

XXXXXXXXXXXXX	
Date: [MONTH XX, 2002]	Facility: [FACILITY]
This checklist covers information that is released to the public via corporate communications, press releases, the Internet, and other means.	
	COMMENTS
What is the required review process for information before it is posted on the Website?	

CHECKLIST F.7 TRASH AND WASTE HANDLING (X)

XXXXXXXXXXXXX	
Date: [MONTH XX, 2002] Facility: [FACILITY]	
This checklist covers the handling of trash and waste that may have security implications (e.g., documents records, discarded equipment)	
	COMMENTS
(a) Responsibilities	
What internal offices or departments are responsible for the security of trash and waste?	
Describe established policies for trash and waste handling?	
(b) Trash Handling	
Where is trash accumulated?	
Is the trash accessible to outsiders?	
Who collects the trash?	
Where is the trash taken?	
(c) Paper Waste Handling	
Where is paper waste accumulated?	
Describe the availability and use of shredders throughout the facility?	
What paper waste is accessible to outsiders?	
Who collects the paper waste?	
Where is the paper waste taken? Is it sent for recycling?	
Describe any on-site destruction of paper waste? How it is protected until destroyed.	
(d) Salvage Material Handling	
Does salvage material (e.g., serviceable equipment no longer needed, surplus equipment) potentially contain sensitive information?	
Describe the procedures for inspecting salvage material before release?	
(e) Dumpster Control	
Describe how dumpsters (for trash, paper waste, and salvage materials) that are accessible to the public are monitored to prevent "dumpster diving?"	

CHECKLIST F.7 TRASH AND WASTE HANDLING (X)

XXXXXXXXXXXXX	
Date: [MONTH XX, 2002] Facility: [FACILITY]	
This checklist covers the handling of trash and waste that may have security implications (e.g., documents records, discarded equipment)	
	COMMENTS
How are publicly accessible dumpsters sampled for sensitive information?	

ATTACHMENT G: INFRASTRUCTURE INTERDEPENDENCIES SURVEY (X)

(X) The objective of the infrastructure interdependencies portion of the survey is to identify infrastructures that support the entire facility and its critical assets and to determine if adequate measures are in place to protect and back up these infrastructures. This attachment contains checklists that are used to collect information for the survey. The first checklist (Checklist G.1) identifies the offices or departments within the facility that are responsible for oversight of the infrastructures and the procedures in place to guide this oversight. The remaining checklists are used for each of the individual infrastructures supporting the facility as a whole and/or each critical asset that has been identified. The conclusion of whether the infrastructures have adequate protection is to be reported as part of the findings in the body of the survey results report (Section 6).

(X) The checklists that are include here are:

G.1 Infrastructure Oversight and Procedures,
G.2 Electric Power Supply and Distribution,
G.3 Petroleum Fuels Supply and Storage,
G.4 Natural Gas Supply,
G.5 Telecommunications,
G.6 Transportation,
G.7 Water and Wastewater,
G.8 Emergency Services,
G.9 Computers and Servers,
G.10 HVAC System,
G.11 Fire Suppression and Fire Fighting System,
G.12 SCADA System,
G.13 Physical Security System, and
G.14 Financial System

(X) A "set" of checklists (G.2 through G.14) should be completed for the facility as a whole and for each of the critical assets within the facility. It may be that some parts of the checklist for certain infrastructures may refer to the checklist of another infrastructure. For example, if an infrastructure has its own electric power supply and distribution system, that system would be included in the checklist for that infrastructure. However, if the infrastructure depends entirely on the asset's or facility's electric power supply and distribution system for its electric power, the checklist for that infrastructure need only reference the appropriate electric power supply and distribution infrastructure checklist. Also, it may be that the checklists for certain infrastructures of some assets may simply refer to the checklist for that infrastructure for the facility as a whole if that infrastructure supports more than one or all of the critical assets.

(X) Checklists of all the infrastructures supporting each asset or facility need not be completed as part of this survey. Only those infrastructures that are important to the asset's or facility's ability to continue to carry out its critical functions and activities need be considered in detail. In addition, the time and resources allotted for the survey may limit the infrastructures that can be examined.

(X) At the end of Attachment G there are lists of questions about the different aspects of each of the 13 infrastructures that are to be used as guidelines to help determine the types of information to be collected in the various sections of each of the checklists (Checklists G.2 through G.14). These questions are separated from the checklists themselves in order to save space.

Not all 13 infrastructures (Checklists G.2 through G.14) will be critical to the functions or activities at either the facility as a whole or at the individual assets considered in the survey. Complete checklists only for those infrastructures that are considered critical and mark the others "Not Considered Critical" or "Not Considered in Survey." The emergency services, computers and servers, and financial system infrastructures generally will not be of primary concern for this survey and can be eliminated if useful information is not readily available

In the case of checklists that apply to individual critical assets that partially make up the entire facility being surveyed, duplicate the checklist and insert the correct asset name [ASSET]. Keep the original checklist number (e.g., CHECKLIST G.4) to maintain the correct link to the portion of the report template into which that information feeds.

CHECKLIST G.1 INFRASTRUCTURE OVERSIGHT AND PROCEDURES (X)

XXXXXXXXXXXX	
Date: [MONTH XX, 2002] Facility: [FACILITY]	
	COMMENTS
(a) Infrastructure Oversight	
Does the facility have a central office or department (such as building management, plant services, facility management) that is responsible for overseeing all or most the infrastructures? Indicate the office/department and list the infrastructures for which they have responsibility and the extent of their responsibilities.	
What coordination or oversight role does the physical security office have in regards to the infrastructures that support critical functions or activities?	
(b) Infrastructure Procedures	
In general, are operating procedures in place for the systems that make up the internal infrastructures and for the physical connections and contracts with the external infrastructures that support them? Describe the extent of these procedures, their format, their availability to relevant staff, and the extent to which they are regularly followed. (Note: details about procedures for specific individual infrastructures are addressed in the relevant checklists.)	

CHECKLIST G.1 INFRASTRUCTURE OVERSIGHT AND PROCEDURES (X)

XXXXXXXXXXXX	
Date: [MONTH XX, 2002] Facility: [FACILITY]	
	COMMENTS
Are contingency procedures in place for the systems that make up the internal infrastructures and for the physical connections and contracts with the external infrastructures that support them? Describe the extent of these procedures, their format, and their availability to relevant staff. (Note: Contingencies refer to situations brought about by a failure or disruption within an infrastructure or the infrastructures that support it.)	
If they exist, have the contingency procedures been tested and are they exercised regularly either as a part of normal operations as through specially designed drills? Describe the drills and their results.	
Are emergency procedures in place for the systems that make up the internal infrastructures and for the physical connections and contracts with the external infrastructures that support them? Describe the extent of these procedures, their format, and their availability to relevant staff. (Note: Emergencies refer to situations brought about external stress on the facility such as high demands.)	
If they exist, have the emergency procedures been tested and are they exercised regularly through specially designed drills? Describe the drills and their results.	

CHECKLIST G.2 ELECTRIC POWER SUPPLY AND DISTRIBUTION (X)

XXXXXXXXXXXXX	
Date: [MONTH XX, 2002]	Facility: [FACILITY]
This checklist applies to [the entire facility/ASSET]	
DESCRIPTION AND COMMENTS	
(a) Primary Source of Electric Power	
(b) Electric Distribution System	
(c) Backup Electric Power Systems	
(d) Commercial Electric Power Sources	
(e) Commercial Electric Power Pathways	
(f) Commercial Electric Power Contracts	
(g) Historical Reliability	

CHECKLIST G.3 PETROLEUM FUELS SUPPLY AND STORAGE (X)

XXXXXXXXXXXXX
Date: [MONTH XX, 2002] Facility: [FACILITY]
This checklist applies to [the entire facility/ASSET]
DESCRIPTION AND COMMENTS
(a) Uses of Petroleum Fuels
(b) Reception Facilities
(c) Supply Contracts

CHECKLIST G.4 NATURAL GAS SUPPLY (X)

XXXXXXXXXXXXX
Date: [MONTH XX, 2002] Facility: [FACILITY]
This checklist applies to [the entire facility/ASSET]
DESCRIPTION AND COMMENTS
(a) Sources of Natural Gas
(b) Pathways of Natural Gas
(c) Natural Gas Contracts
(d) Historical Reliability

CHECKLIST G.5 TELECOMMUNICATIONS (X)

XXXXXXXXXXXXX
Date: [MONTH XX, 2002] Facility: [FACILITY]
This checklist applies to [the entire facility/ASSET]
Note: Includes internal communications (voice, FAX, intranet, data transfer, e-mail), microwave/radio communications, and Internet and commercial communications.
DESCRIPTION AND COMMENTS
(a) Internal Telephone System
(b) Data Transfer
(c) Cellular/Wireless/Satellite Systems
(d) Intranet and E-mail System
(e) Redundant Access to Intranet and E-mail System
(f) On-site Fixed Components of Microwave/Radio System
(g) Mobile and Remote Components of Microwave/Radio System
(h) Commercial Telecommunications Carriers
(i) Pathways of Commercial Telecommunications Cables
(j) Historical Reliability of Commercial Carriers
(k) Backup Communications Systems

CHECKLIST G.6 TRANSPORTATION (X)

XXXXXXXXXXXXX
Date: [MONTH XX, 2002] Facility: [FACILITY]
This checklist applies to [the entire facility/ASSET]
Note: Includes road, rail, air, water, and pipeline.
DESCRIPTION AND COMMENTS
(a) Road Access
(b) Road Access Control
(c) Rail Access
(d) Rail Access Control
(e) Airports and Air Routes
(f) Waterway Access
(g) Waterway Access Control
(h) Pipeline Access
(i) Pipeline Access Control

CHECKLIST G.7 WATER AND WATER SYSTEM (X)

XXXXXXXXXXXX
Date: [MONTH XX, 2002] Facility: [FACILITY]
This checklist applies to [the entire facility/ASSET]
DESCRIPTION AND COMMENTS
(a) Primary Domestic Water System
(b) Domestic Water Supply
(c) Backup Domestic Water System
(d) Primary Industrial Water System
(e) Industrial Water Supply
(f) Backup Industrial Water System
(g) Primary Industrial Wastewater System
(h) Backup Wastewater System
(i) Commercial/Public Water Supply Reliability
(j) Commercial/Public Wastewater System Reliability

CHECKLIST G.8 EMERGENCY SERVICES (X)

XXXXXXXXXXXXX
Date: [MONTH XX, 2002] Facility: [FACILITY]
This checklist applies to [the entire facility/ASSET]
Note: This infrastructure area is not of primary concern for this survey and can be eliminated if useful information is not readily available.
DESCRIPTION AND COMMENTS
(a) Local Police
(b) County/State Police
(c) Federal Bureau of Investigation (FBI)
(d) Fire Department
(e) Emergency Medical Services

CHECKLIST G.9 INTERNAL COMPUTERS AND SERVERS (X)

XXXXXXXXXXXXX
Date: [MONTH XX, 2002] Facility: [FACILITY]
This checklist applies to [the entire facility/ASSET]
Note: This infrastructure area is not of primary concern for this survey and can be eliminated if useful information is not readily available.
DESCRIPTION AND COMMENTS
(a) Electric Power Sources
(b) Environmental Control
(c) Protection

CHECKLIST G.10 HVAC SYSTEM (X)

XXXXXXXXXXXXX
Date: [MONTH XX, 2002] Facility: [FACILITY]
This checklist applies to [the entire facility/ASSET]
Note: Includes air handlers, heating plants, cooling towers, and chillers.
DESCRIPTION AND COMMENTS
(a) Primary HVAC System
(b) Supporting Infrastructure
(c) Backup HVAC Systems

CHECKLIST G.11 FIRE SUPRESSION AND FIRE FIGHTING SYSTEM (X)

XXXXXXXXXXXXX
Date: [MONTH XX, 2002] Facility: [FACILITY]
This checklist applies to [the entire facility/ASSET]
DESCRIPTION AND COMMENTS
(a) Alarms
(b) Fire Suppression
(c) Fire Fighting
(d) Other Systems

CHECKLIST G.12 SCADA SYSTEM (X)

XXXXXXXXXXXXX
Date: [MONTH XX, 2002] Facility: [FACILITY]
This checklist applies to [the entire facility/ASSET]
DESCRIPTION AND COMMENTS
(a) Type of System
(b) Control Centers
(c) Electric Power Sources
(d) Communications Pathways
(e) Remote Components
(f) Dedicated SCADA Computers and Servers

CHECKLIST G.13 PHYSICAL SECURITY SYSTEM (X)

XXXXXXXXXXXXX
Date: [MONTH XX, 2002]   Facility: [FACILITY]
This checklist applies to [the entire facility/ASSET]
DESCRIPTION AND COMMENTS
(a) Electric Power Sources
(b) Communications Pathways
(c) Computer Support

CHECKLIST G.14 FINANCIAL SYSTEM (X)

XXXXXXXXXXXXX
Date: [MONTH XX, 2002] Facility: [FACILITY]
This checklist applies to [the entire facility/ASSET]
Note: This infrastructure area (includes monetary transactions) is not of primary concern for this survey and can be eliminated if useful information is not readily available.
DESCRIPTION AND COMMENTS
(a) Electric Power Sources
(b) Communications Pathways
(c) Computer Support

CHECKLIST CONSIDERATIONS: INTERDEPENDENCIES SURVEY (X)

(X) This section contains questions related to each of the infrastructure interdependency survey checklists and their subsections. These questions are intended for use by the survey teams during preparations for interviews with facility representatives to help assure that all relevant aspects of the critical infrastructures are considered in the survey.

(X) (a) Electric Power Supply and Distribution

(X) Primary Source of Electric Power

(X)
- If the primary source of electric power is a commercial source, are there multiple independent feeds? If so, describe the feeds and their locations.

(X)
- If the primary source of electric power is a system operated by the facility or asset, what type of system is it?

(X)
- If a facility operated primary electric generation system is used, what is the fuel or fuels used?

(X)
- If petroleum fuel is used, what quantity of fuel is stored on site for the primary electric generation system and how long it will last under different operating conditions?

(X)
- If the fuel is stored on site, are arrangements and contracts in place for resupply and management of the fuel?

(X) Electric Distribution System

(X)
- Are the components of the electric system that are located outside of buildings (such as generators, fuel storage facilities, transformers, transfer switches) protected from vandalism or accidental damage by fences or barriers? If so, describe the type of protection and level of security it provides.

(X)
- Are the various sources of electric power and the components of the internal electric distribution systems such that they may be isolated for maintenance or replacement without affecting the critical functions of the asset/facility? If not, describe the limitations.

(X)
- Have any single points of failure been identified for the electrical power supply and distribution system? If so, list them and describe.

(X) Backup Electric Power Systems

(X) • Are there additional emergency sources of electric supply beyond the primary system (such as multiple independent commercial feeds, backup generators, uninterruptible power supply [UPSs])? If there are, describe them.

(X) • If there is a central UPS, does it support all the critical functions of the asset/facility in terms of capacity and connectivity? Specify for how long it can operate on battery power and list any potentially critical functions that are not supported.

(X) • If there is a backup generator system, does it support all the critical functions of the facility in terms of capacity and connectivity? Specify the fuel and list any potentially critical functions that are not supported.

(X) • Is the fuel for the backup generator system a petroleum fuel? If yes, specify the quantity stored on site and how long it will last.

(X) • If the fuel is stored on site, are arrangements and contracts in place for resupply and management of the fuel?

(X) Commercial Electric Power Sources

(X) • How many substations feed the area of the asset/facility and the asset/facility itself? That is, is the area supplied by multiple substations? If more than one, which ones have sufficient individual capacities to supply the critical needs of the asset/facility?

(X) • How may distinct independent transmission lines supply the substations? Indicate if an individual substation is supplied by more than one transmission line and which substations are supplied by independent transmission lines.

(X) Commercial Electric Power Pathways

(X) • Are the power lines into the area of the asset/facility and into the asset/facility itself above ground (on utility poles), buried, or a combination of both? If both, indicate locations of portions above ground.

(X) • Do the power lines from these substations follow independent pathways to the area of the asset/facility? If not, specify how often and where they intersect or follow the same corridor.

(X) • Are the paths of the power lines co-located with the rights-of-way of other infrastructures? If yes, indicate how often and where they follow the same rights-of-way and the infrastructures that are co-located.

(X) • Are the paths of the power lines located in areas susceptible to natural or accidental damage (such as overhead lines near highways; power lines across bridges, dams, or landslide areas)? If yes, indicate the locations and types of potential disruptions.

(X) Commercial Electric Power Contracts

(X) • What type of contract does the asset/facility have with the electric power distribution company or transmission companies? Specify the companies involved and whether there is a direct physical link (distribution or transmission power line) to each company.

(X) • If there is an interruptible contract (even in part), what are the general conditions placed up interruptions such as the minimum quantity that is not interruptible, the maximum number of disruptions per time period, and the maximum duration of disruptions? Has electric service been interrupted in the past? If yes, describe the circumstances and any effect the outages have had on the critical functions and activities of the asset/facility.

(X) Historical Reliability

(X) • Historically, how reliable has the commercial electric power been in the area? Quantify in terms of annual number of disruptions and their durations.

(X) • Typically, when power outages occur, are they of significant duration (as opposed to just a few seconds or minutes)? Quantify the duration of the outages.

(X) • Have there ever been electric power outages of sufficient frequency and duration so as to affect the critical functions and activities of the asset/facility?

(X) (b) Petroleum Fuels Supply and Storage

(X) Uses of Petroleum Fuels

(X) • Are petroleum fuels used in normal operations at the asset/facility? If yes, specify the types and uses.

(X) • Are petroleum fuels used during contingency or emergency operations such as for backup equipment or repairs? If yes, specify the types of fuels and their uses.

(X) Reception Facilities

(X) • How are the various petroleum fuels normally delivered to the asset/facility? Indicate the delivery mode and normal frequency of shipments for each fuel type.

(X) • Under maximum use-rate conditions, are their sufficient reception facilities (truck racks, rail sidings, surge tank capacity, barge moorings) to keep up with maximum contingency or emergency demand)? If no, explain where the expected shortfalls would be and their impacts.

(X) • Are the petroleum fuel delivery pathways co-located with the rights-of-way of other infrastructures or located in areas susceptible to natural or accidental damage (across bridges or dams, in earthquake or landslide areas)? If yes, indicate the locations and types of potential disruptions.

(X) • Are contingency procedures in place to allow for alternative modes or routes of delivery? If yes, describe these alternatives and indicate whether they have sufficient capacity to fully support the critical functions and activities of the asset/facility

(X) Supply Contracts

(X) • Are contracts in place for the supply of petroleum fuels? Specify the contractors, the types of contracts, the modes of transport (pipeline, rail car, tank truck), and the frequency of normal shipments.

(X) • Are arrangements for emergency deliveries of petroleum fuels in place? Indicate the basic terms of the contracts in terms of the maximum time to delivery and the minimum and maximum quantity per delivery. Also, indicate if these terms as such that there may be effects on the critical functions and activities of the asset/facility.

(X) (c) Natural Gas Supply

(X) Sources of Natural Gas

(X) • How many city gate stations supply the natural gas distribution system in the area of the asset/facility and the asset/facility itself? If more than one, which ones are critical to maintaining the distribution system?

(X) • How may distinct independent transmission pipelines supply the city gate stations? Indicate if an individual gate station is supplied by more than one transmission pipeline and which stations are supplied by independent transmission pipelines.

(X) Pathways of Natural Gas

(X) • Do the distribution pipelines from the individual city gate stations follow independent pathways to the area of the asset/facility? If not, specify how often and where they intersect or follow the same corridor.

(X) • Are the paths of the pipelines co-located with the rights-of-way of other infrastructures? If yes, indicate how often and where they follow the same rights-of-way and the infrastructures that are co-located.

(X) • Are the paths of the pipelines located in areas susceptible to natural or accidental damage (such as across bridges or dams, in earthquake or landslide areas)? If yes, indicate the locations and types of potential disruptions.

(X) • Is the local distribution system well integrated (i.e., can gas readily get from any part of the system to any other part of the system)?

(X) Natural Gas Contracts

(X) • Does the asset/facility have a firm delivery contract, an interruptible contract, or a mixed contract with the natural gas distribution company or the transmission companies? Specify the companies involved and whether there is a direct physical link (pipeline) to each company.

(X) • If there is an interruptible contract (even in part), what are the general conditions placed up interruptions such as the minimum quantity that is not interruptible, the maximum number of disruptions per time period, and the maximum duration of disruptions? Has natural gas service been interrupted in the past? If yes, describe the circumstances and any effect the outages have had on the critical functions and activities of the asset/facility.

(X) • Does the asset/facility have storage or some other sort of special contracts with natural gas transmission or storage companies? If yes, briefly describe the effect on sustaining a continuous supply of natural gas to the asset/facility.

(X) • In case of a prolonged disruption of natural gas supply, are contingency procedures in place to allow for the use of alternative fuels (such as on-site propane-air, liquefied petroleum gas, or petroleum fuels)? If yes, describe these alternatives and indicate whether they have sufficient capacity to fully support the critical functions and activities of the asset/facility

(X) Historical Reliability

(X) • Historically, how reliable has the natural gas supply been in the area? Quantify by describing any unscheduled or unexpected disruptions. Were there any effects on the critical functions and activities of the asset/facility?

(X) • If operating under an interruptible service agreement, has natural gas service ever been curtailed? If yes, how often, for how long, and were there any effects on the critical functions and activities of the asset/facility?

(X) (d) Telecommunications

(X) Internal Telephone System

(X) • What types of telephone systems are used within the asset/facility? Are there multiple independent telephone systems? Specify the types of systems, their uses, and whether they are copper-wire or fiber-optic based.

(X) • If there are there multiple independent telephone systems within the asset/facility, is each one adequate to support the critical functions and activities? Indicate any limitations.

(X) • If there are multiple (from independent systems) or redundant (from built-in backups) switches and cables, are they physically separated and isolated to avoid common causes of failure?

(X) • Are the telephone switches located in limited-access or secured areas away from potential damage due to weather or water leaks? Specify types of protection provided.

(X) Data Transfer

(X) • For large volume and high-speed data transfer within the asset/facility, is there a separate system of switches and cables with in the asset/facility? Specify the type of systems and whether it is copper-wire or fiber-optic based.

(X) • If there is a separate system for large volume and high-speed data transfer, are there redundant switches and cables. If yes, describe the situation.

(X) • If there are redundant switches and cables, are they physically separated and isolated to avoid common causes of failure?

(X) • Are the data-transfer switches located in limited-access or secured areas away from potential damage due to weather or water leaks? Specify the types of protection provided.

(X) Cellular/Wireless/Satellite Systems

(X) • Are cellular/wireless telephones and pagers in widespread use within the asset/facility? If yes, briefly describe their uses.

(X) • If cellular/wireless telephones and pagers are in widespread use, are they adequate to support the critical functions and activities? Specify any limitations.

(X) • Are satellite telephones or data links in widespread use within the asset/facility? If yes, briefly describe their uses.

(X) • If satellite telephones or data links are in widespread use, are they adequate to support the critical functions and activities? Specify any limitations.

(X) Intranet and E-mail System

(X) • Is the asset's/facility's intranet and e-mail system dependent on the asset's/facility's computers and servers? If yes, describe the dependence.

(X) • Is the asset's/facility's intranet and e-mail system dependent on the asset's/facility's telephone system? If yes, describe the dependence.

(X) • If the asset's/facility's intranet and e-mail system is a separate system, are there provisions within the asset's/facility's primary electric power supply and distribution system to supply power for the intranet and e-mail system? If yes, specify under what conditions and for how long.

(X) • If the asset's/facility's intranet and e-mail system is a separate system, does it have its own backup electric power supply, such as local UPSs? If yes, specify the type and how long it can operate.

(X) • If the asset's/facility's intranet and e-mail system is a separate system, does the asset's/facility's central HVAC system provide environmental control for important components or does it have its own independent environmental control system? If it has its own, specify the type.

(X) • If the asset's/facility's intranet and e-mail system is a separate system, can it operate with a loss of all environmental control? If yes, specify for how long under various conditions.

(X) • If the asset's/facility's intranet and e-mail system is a separate system, are there any backup environmental controls explicitly for the system? If yes, indicate the type of backup and the expected maximum duration of operation.

(X) • If the asset's/facility's intranet and e-mail system is a separate system, is there special physical security provided for the important components? If yes, specify the type of security and the level of protection provided.

(X) • If the asset's/facility's intranet and e-mail system is a separate system, is there special fire suppression equipment for the important components such as Halon, Inergen, inert gases, or carbon dioxide? If yes, specify the type of system.

(X) • If the asset's/facility's intranet and e-mail system is a separate system, are there special features or equipment in the area of the important components to limit flooding or water intrusion? If yes, indicate the precautions taken.

(X) • If the asset's/facility's intranet and e-mail system is a separate system, are there alarms for the area of the important components for such things as unauthorized intrusion, loss of electric power, loss of environmental control, fire, and flooding or water intrusion? If yes, specify the types of alarms, how they are monitored, and the response procedure.

(X) Redundant Access to Intranet and E-mail System

(X) • Does the asset/facility have a backup or redundant intranet and e-mail system? If yes, describe the system and the amount of backup it provides.

(X) • Do areas where critical functions and activities take place have multiple or redundant access to the intranet and e-mail system?

(X) • If there are multiple access routes, is each one adequate to support the critical functions and activities? If not, specify any limitations.

(X) On-site Fixed Components of Microwave/Radio System

(X) • Are there multiple or redundant radio communications systems in place within the asset/facility? If yes, specify the types of systems and their uses.

(X) • If there are multiple radio communications systems, is more than one system adequate to support all the critical functions and activities of the asset/facility? Specify any limitations.

(X) • Are there provisions within the asset's/facility's primary electric power supply and distribution system to supply power for the radio communications systems? If yes, indicate under what conditions and for how long.

(X) • Do the radio communications systems have their own backup electric power supply? If yes, specify the type and how long it can operate.

(X) • Are the components of the system located outside of buildings (such as antennae, on-site towers) protected from vandalism or accidental damage by fences or barriers? If protected, specify the types of protection and level of security they provide.

(X) Mobile and Remote Components of Microwave/Radio System

(X) • Are there mobile components to the radio communications system (such as on vehicles or vessels)? If yes, describe the mobile components.

(X) • Are the mobile components of the radio communications system protected from vandalism or accidental damage by locked boxes or lockable vehicle cabs? Specify the types of protection and level of security they provide.

(X) • Are there remote components to the radio communications system (such as relay towers)? If yes, describe them and their uses.

(X) • Are there backup sources of electric power for these remote components? If yes, indicate the type of backup, the fuels used, and the expected length of operations.

(X) • Are there environmental controls required for the remote components (such as heating, cooling)? If yes, describe them.

(X) • Are there backup environmental controls for these remote components? If yes, indicate the type of backup, the fuels used, and the expected length of operations.

(X) • Is physical security provided for the remote components of the radio communications system? If yes, specify the types of security and the level of protection provided.

(X) • Are there alarms at the remote components of the radio communications system for such things as intrusion, loss of electric power, loss of environmental control, and fuel reserves? If yes, specify the types of alarms, how they are monitored, and the response procedure.

(X) Commercial Telecommunications Carriers

(X) • Are there multiple telecommunications carriers used by the asset/facility (possibly commercial, contracted, or organization-owned)? List them, specify the service they provide or the type of information carried (such as analog telephone voice and FAX, digital telephone voice, Internet connections, dedicated data transfer), and the type of media used (copper cable, fiber-optic cable, microwave, satellite

(X) Pathways of Commercial Telecommunications Cables

(X) • Are the telecommunications cables into the area of the asset/facility and into the asset/facility itself above ground (on utility poles), buried, or a combination of both? If both, indicate locations of portions above ground.

(X) • Do the telecommunications cable follow independent pathways into the area of the asset/facility and into the asset/facility itself? If not, indicate how independent they are (some common corridors, intersect at one or more points).

(X) • Are the paths of the telecommunications cables co-located with the rights-of-way of other infrastructures? If yes, describe the extent of the co-location and indicate the other infrastructures.

(X) • Are the paths of the telecommunications cables located in areas susceptible to natural or accidental damage (such as overhead cables near highways; cables across bridges, dams, or landslide areas)? If yes, indicate the locations and types of potential disruptions.

(X) • Do the various telecommunications carriers and cable pathways use separate independent end offices (EO), access tandems (AT), points of presence (POP), and network access points (NAP) to reach the communications transmission backbones? Briefly describe the extent of this independence.

(X) Historical Reliability of Commercial Carriers

(X) • Historically, has the public switched network (PSN) telephone system in the area been reliable? Quantify in terms of number of both complete outages and dropped connections.

(X) • Typically, when telephone outages occur, are they of significant duration (as opposed to just a few seconds or minutes)? Quantify in terms of potential effects on the critical functions and activates at the asset/facility.

(X) • Historically, have the Internet and dedicated data transfer systems in the area been reliable? Quantify in terms of number of both complete outages and dropped connections.

(X) • Typically, when Internet or data transfer connectivity outages or disruptions occur, are they of significant duration (as opposed to just a few seconds or minutes)? Quantify in terms of potential effects on the critical functions and activates at the asset/facility.

(X) Backup Communications Systems

(X) • Are there redundant or backup telephone systems in place if the primary system is disrupted? Specify the extent to which the secondary systems can support the critical functions and activities at the asset/facility.

(X) • Are there redundant or backup Internet and dedicated data transfer systems in place if the primary systems are disrupted? Specify the extent to which the secondary systems can support the critical functions and activities at the asset/facility.

(X) (e) Transportation

(X) Road Access

(X) • Are there multiple roadways into the area of the asset/facility from the major highways and interstates? Describe the route or routes and indicate any load or throughput limitations with respect the needs of the asset/facility.

(X) • Are there any choke points or potential hazard areas along these roadways such as tunnels, bridges, dams, low-lying fog areas, landslide areas, or earthquake faults? Describe the constrictions or hazards and indicate if, historically, closures have occurred somewhat regularly.

(X) Road Access Control

(X) • Could intruders or others determined to do damage to the asset/facility gain access to the asset/facility or nearby areas by road without being readily identified and controlled? If yes, describe the means of access and indicate any limitations on the number of people, the size and number of vehicles, and the size or quantity of material that could approach the asset/facility by road.

(X) • Are there uncontrolled parking lots or open areas for parking near the facility where vehicles could park without drawing significant attention? If yes, indicate the number of vehicles and the size or types of vehicles that would begin to be noticed.

(X) Rail Access

(X) • Are there multiple rail routes into the area of the asset/facility from the nearby rail yards or switchyards? Describe the route or routes and indicate any load or throughput limitations with respect the needs of the asset/facility.

(X) • Are there any choke points or potential hazard areas along these rail rights-of-way such as tunnels, bridges, dams, landslide areas, or earthquake faults? Describe the constrictions or hazards and indicate if, historically, rail traffic closures have occurred somewhat regularly.

(X) • Is there sufficient rail siding space at or near the asset/facility to accommodate rail cars if the number of incoming cars exceeds normal expectations or if outgoing cars are not picked up as normally scheduled? Indicate the magnitude of this excess capacity in terms of the time period before the critical functions or activities of the asset/facility would be affected.

(X) Rail Access Control

(X) • Could intruders or others determined to do damage to the asset/facility gain access to the asset/facility or nearby areas by rail without being readily identified and controlled? If yes, describe the means of access and indicate any limitations on the number of people and rail cars that could approach the asset/facility by rail.

(X) • Are there railroad tracks or sidings near the asset/facility where rail cars could be positioned without drawing significant attention? If yes, indicate the number and the types of rail cars that would begin to be noticed.

(X) Airports and Air Routes

(X) • Are there multiple airports the area of the site of sufficient size and with sufficient service to support the critical functions and activities at the asset/facility? Enumerate the airports and indicate any limitations.

(X) • Are there any regular air routes that pass over or near the asset/facility that could present a danger to the asset/facility if there were some sort of an air disaster? Record any concerns.

(X) Waterway Access

(X) • Are there multiple water routes to the ports, harbors, or landings used by the asset/facility from the open ocean or major waterway? Describe the route or routes and indicate any load, draft, beam, or throughput limitations with respect the needs of the organization.

(X) • Are there any choke points or potential hazard areas along these waterways such as bridges, draw or lift bridges, locks and dams, low-lying fog areas, or landslide areas? Describe the constrictions or hazards and indicate if, historically, closures have occurred somewhat regularly.

(X) • Is there sufficient mooring, wharf, or dock space at the ports, harbors, or landings used by the asset/facility to accommodate ships or barges if the number of incoming vessels exceeds normal expectations or if outgoing barges are not picked up as normally scheduled? Indicate the magnitude of this excess capacity in terms of the time period before the critical functions or activities at the asset/facility would be affected.

(X) Waterway Access Control

(X) • Could intruders or others determined to do damage to the asset/facility gain access to the asset/facility or nearby areas by water without being readily identified and controlled? If yes, describe the means of access and indicate any limitations on the number of people, the size and number of vessels, and the size or quantity of material that could approach the asset/facility by water.

(X) • Are there uncontrolled docks or mooring areas near the asset/facility or the ports, harbors, or landings used by the asset/facility where vessels could moor without drawing significant attention? If yes, indicate the number of vessels and the size or types of vessels that would begin to be noticed.

(X) Pipeline Access

(X) • What materials, feedstocks, or products (such as crude oil, intermediate petroleum products, refined petroleum products, or liquefied petroleum gas—do not include water, wastewater, or natural gas unless there are special circumstances related to these items) are supplied to or shipped from the asset/facility by way of pipeline transportation?

(X) • Are there multiple pipelines and pipeline routes into the area of the asset/facility from major interstate transportation pipelines? If yes, indicate which pipelines or combinations of pipelines have sufficient capacity to serve the asset/facility

(X) • List the pipeline owners/operators, indicate the types of service provided (dedicated or scheduled shipments), describe the route or routes, and indicate any capacity limitations with respect the needs of the asset/facility.

(X) • Are there any bottlenecks or potential hazard areas along these pipeline or pipeline routes such as interconnects, terminals, tunnels, bridges, dams, landslide areas, or earthquake faults? Describe the constrictions or hazards and indicate if, historically, outages or delays have occurred somewhat regularly.

(X) Pipeline Access Control

(X) • Could intruders or others determined to bring down the asset/facility gain access to the pipeline near the asset/facility or elsewhere along the pipeline route? Describe the protective measures that are in place and indicate any pipeline segments or facilities (such as pump stations, surge tanks) of concern.

(X) (f) Water and Wastewater

(X) Primary Domestic Water System

(X) • Does the asset/facility have a domestic water system? If yes, specify the uses of the water (such as restrooms, locker rooms, kitchens, HVAC makeup water).

(X) • Does the water supply for the domestic water system come from an external source (such as community, city, or regional water mains) or from an internal system (such as wells, river, or reservoir)? If internal, describe the system.

(X) Domestic Water Supply (external)

(X) • What type of external water supply system provides the domestic water? Indicate whether it is public or private and its general size (such as community, city, or regional).

(X) • Are on-site pumps and/or storage tanks used to boost the pressure or provide for periods of peak usage? If yes, briefly describe them and their purpose.

(X) • Are the on-site booster water pumps normally dependent upon the asset's/facility's primary electric power supply and distribution system?

(X) • Are there multiple sources of electric supply (such as multiple independent commercial feeds, backup generators, UPSs) explicitly for the on-site booster water pumps? If yes, specify them.

(X) • If there is a special UPS, can is support the on-site booster pumps at required levels? Specify for how long it can operate on battery power.

(X) • If there is a special backup generator system, can is support the on-site booster pumps at required levels? Also indicate the type of fuel or fuels used.

(X) • If the fuel for the dedicated backup generator system for the booster pumps is a petroleum fuel, indicate the quantity stored on site and how long it will last.

(X) • If the fuel for the dedicated backup generator for the booster pumps is stored on site, are arrangements and contracts in place for resupply and management of the fuel?

(X) Domestic Water Supply (internal)

(X) • Indicate the source of the water (such as wells, river, or reservoir), the adequacy of the supply's capacity, and whether it is gravity feed or requires active pumps (generally electric).

(X) • Are the on-site domestic water system pumps independent of the asset's/facility's primary electric power supply and distribution system?

(X) • Are there multiple sources of electric supply (such as multiple independent commercial feeds, backup generators, UPSs) explicitly for the on-site domestic water system pumps? If yes, specify them.

(X) • If there is a special UPS, can is support the on-site domestic water system pumps at required levels? Specify for how long it can operate on battery power.

(X) • If there is a special backup generator system, can is support the on-site domestic water system pumps at the required levels? Also indicate the type of fuel or fuels used.

(X) • If the fuel for the dedicated backup generator system for the on-site domestic water system pumps is a petroleum fuel, indicate the quantity stored on site and how long it will last. Are arrangements and contracts in place for resupply and management of the fuel?

(X) Backup Domestic Water System

(X) • Is there an independent backup water source to the primary domestic supply system? If yes, specify the type of backup system (such as wells, river, reservoir, tank truck), describe the specific source of the water, indicate the adequacy of the backup supply's capacity, and indicate if it is gravity feed or requires active pumps (generally electric).

(X) • Are the independent backup water source system pumps independent of the asset's/facility's primary electric power supply and distribution system?

(X) • Are there multiple sources of electric supply (such as multiple independent commercial feeds, backup generators, UPSs) explicitly for the backup water source system pumps? If yes, specify them.

(X) • If there is a special UPS, can is support the backup domestic water source pumps at the required levels? Specify for how long it can operate on battery power.

(X) • If there is a special backup generator system, can it support the backup domestic water source system pumps at the required levels? Also indicate the type of fuel or fuels used.

(X) • If the fuel for the dedicated backup generator system for the backup water source system pumps is a petroleum fuel, indicate the quantity stored on site and how long it will last. Are arrangements and contracts in place for resupply and management of the fuel?

(X) Primary Industrial Water System

(X) • Does the asset/facility have an industrial water system? If yes, specify the uses of the water (such as wash water, process water, generation of process steam, cooling).

(X) • Does the water supply for the industrial water system come from an external source (such as community, city, or regional water mains) or from an internal system (such as wells, river, or reservoir)? If internal, describe the system.

(X) Industrial Water Supply (internal)

(X) • What type of external water supply system provides the industrial water? Indicate whether it is public or private and its general size (such as community, city, or regional).

(X) • Are on-site pumps and/or storage tanks used to boost the pressure or provide for periods of peak usage? If yes, briefly describe them and their purpose.

(X) • Are the on-site booster water pumps for the industrial water system independent of the asset's/facility's primary electric power supply and distribution system?

(X) • Are there multiple sources of electric supply (such as multiple independent commercial feeds, backup generators, UPSs) explicitly for the on-site booster water pumps? If yes, specify them.

(X) • If there is a special UPS, can it support the on-site booster pumps at required levels? Specify for how long it can operate on battery power.

(X) • If there is a special backup generator system, can it support the on-site booster pumps at required levels? Also indicate the type of fuel or fuels.

(X) • If the fuel for the dedicated backup generator system for the booster pumps is a petroleum fuel, indicate the quantity stored on site and how long it will last. Are arrangements and contracts in place for resupply and management of the fuel?

(X) Industrial Water Supply (external)

(X) • Indicate the source of the water (such as wells, river, or reservoir), the adequacy of the supply's capacity, and whether it is gravity feed or requires active pumps (generally electric).

(X) • Are the on-site industrial water system pumps independent of the asset's/facility's primary electric power supply and distribution system?

(X) • Are there multiple sources of electric supply (such as multiple independent commercial feeds, backup generators, UPSs) explicitly for the on-site industrial water system pumps? If yes, specify them.

(X) • If there is a special UPS, can is support the on-site industrial water system pumps at required levels? Specify for how long it can operate on battery power.

(X) • If there is a special backup generator system, can it support the on-site industrial water system pumps at the required levels? Also indicate the type of fuel or fuels.

(X) • If the fuel for the dedicated backup generator system for the on-site industrial water system pumps is a petroleum fuel, indicate the quantity stored on site and how long it will last. Are arrangements and contracts in place for resupply and management of the fuel?

(X) Backup Industrial Water System

(X) • Is there an independent backup water source to the primary industrial water supply system? If yes, specify the type of backup system (such as wells, river, reservoir, tank truck), describe the specific source of the water, indicate the adequacy of the backup supply's capacity, and indicate if it is gravity feed or requires active pumps (generally electric).

(X) • Are the independent backup water source system pumps independent of the asset's/facility's primary electric power supply and distribution system?

(X) • Are there multiple sources of electric supply (such as multiple independent commercial feeds, backup generators, UPSs) explicitly for the backup water source system pumps? If yes, specify them.

(X) • If there is a special UPS, can is support the backup industrial water source pumps at the required levels? Specify for how long it can operate on battery power.

(X) • If there is a special backup generator system, can is support the backup industrial water source system pumps at required levels? Also indicate the type of fuel or fuels.

(X) • If the fuel for the dedicated backup generator system for the backup water source system pumps is a petroleum fuel, indicate the quantity stored on site and how long it will last. Are arrangements and contracts in place for resupply and management of the fuel?

(X) Primary Industrial Wastewater System

(X) • Does the asset/facility have an on-site industrial wastewater system? If yes, specify the types of wastewater that are processed and the processes used.

(X) • Are the on-site industrial wastewater lift pumps independent of the asset's/facility's primary electric power supply and distribution system?

(X) • Are there multiple sources of electric supply (such as multiple independent commercial feeds, backup generators, UPSs) explicitly for the on-site industrial wastewater lift pumps? If yes, specify them.

(X) • If there is a special UPS, can is support the on-site industrial wastewater lift pumps at required levels? Specify for how long it can operate on battery power.

(X) • If there is a special backup generator system, can it support the on-site industrial wastewater lift pumps at the required levels? Also indicate the type of fuel or fuels.

(X) • If the fuel for the dedicated backup generator system for the on-site industrial wastewater lift pumps is a petroleum fuel, indicate the quantity stored on site and how long it will last. Are arrangements and contracts in place for resupply and management of the fuel?

(X) Backup Wastewater System

(X) • Is there an independent backup system that can be used to handle the industrial wastewater? If yes, specify the type of backup system (such as a redundant system, holding ponds, temporary discharge of unprocessed wastewater), describe the specific process, indicate the adequacy of the backup's capacity and any limitations on how long it can operate, and indicate if it is gravity feed or requires active lift pumps (generally electric).

(X) • Are of the independent backup lift pumps independent of the asset's/facility's primary electric power supply and distribution system?

(X) • Are there multiple sources of electric supply (such as multiple independent commercial feeds, backup generators, UPSs) explicitly for the backup wastewater lift pumps? If yes, specify them.

(X) • If there is a special UPS, can is support the backup industrial wastewater system at the required levels? Specify for how long it can operate on battery power.

(X) • If there is a special backup generator system, can is support the backup industrial wastewater lift pumps at required levels? Also indicate the type of fuel or fuels.

(X) • If the fuel for the dedicated backup generator system for the backup wastewater lift pumps is a petroleum fuel, indicate the quantity stored on site and how long it will last. Are arrangements and contracts in place for resupply and management of the fuel?

(X) Commercial/Public Water Supply Reliability

(X) • Historically, has the city water supply in the area been reliable and adequate? Quantify the reliability and specify any shortfall in the supply pressure or flow rate.

(X) • Typically, when disruptions in the city water supply occur, are they of significant duration (as opposed to just a few hours)? Quantify in terms of potential effects on the critical functions and activities at the asset/facility.

(X) Commercial/Public Wastewater System Reliability

(X) • Historically, has the public wastewater system in the area been reliable and adequate? Quantify the reliability and specify any shortfall in the capacity of the system.

(X) • Typically, when disruptions in the public wastewater system occur, are they of significant duration (as opposed to just a few hours)? Quantify in terms of potential effects on the critical functions and activities at the asset/facility.

(X) • Are there and contingency plans or procedures in place to handle domestic wastewater from the asset/facility if the public system is temporarily unable to accept the waste? If yes, describe them and mention any limitations on quantity of wastewater and duration of outage that might affect the ability of the asset/facility to carry out critical functions or activities.

(X) (g) Emergency Services (Police, Fire, Emergency Medical)

(X) Local Police

(X) • How are the local police involved in protecting the asset/facility?

(X) • What are typical response times and response capabilities?

(X) • Have they provided services in the past? Has their response been helpful?

(X) County/State Police

(X) • How are the county/state police involved in protecting the asset/facility?

(X) • What are typical response times and response capabilities?

(X) • Have they provided services in the past? Has their response been helpful?

(X) Federal Bureau of Investigation (FBI)

(X) • How is the FBI involved in protecting the asset/facility?

(X) • What are typical response times and response capabilities?

(X) • Has the FBI provided services in the past? Has their response been helpful?

(X) **Fire Department**

(X) • How is the local fire department involved in protecting the asset/facility?

(X) • Do they provide inspection and/or certification services?

(X) • What are typical response times and response capabilities?

(X) • Have they provided services in the past? Has their response been helpful?

(X) Emergency Medical Services

(X) • How is the local emergency medical or ambulance service involved in protecting/treating the personnel at the asset/facility?

(X) • Do they provide inspection and/or certification services?

(X) • What are typical response times and response capabilities?

(X) • Have they provided services in the past? Has their response been helpful?

(X) (h) Computers and Servers (Mainframes, Firewalls, Router Equipment)

(X) Electric Power Sources

(X) • Are there provisions within the asset's/facility's primary electric power supply and distribution system to supply power for the computers and servers? If yes, indicate under what conditions and for how long.

(X) • Do the computers and servers have their own backup electric power supply (such as local UPSs or generators)? If yes, specify the types of backup and how long they can operate.

(X) Environmental Control

(X) • Does the asset's/facility's central HVAC system provide environment control to the computer and server areas or do the computer and server areas have their own independent environmental control system? If they have their own system, specify the type.

(X) • Can the computers and servers operate with a loss of all environmental control? If yes, specify for how long under various conditions.

(X) • Are there any backup environmental controls explicitly for the computer and server areas? If yes, indicate the type of backup and the expected maximum duration of operation.

(X) Protection

(X) • Is there special physical security provided for the computer and server areas? If yes, specify the type of security and the level of protection provided.

(X) • Is there special fire suppression equipment in the computer and server areas such as Halon, Inergen, inert gases, or carbon dioxide? If yes, specify the type.

(X) • Are there special features or equipment in the computer and server areas to limit flooding or water intrusion? If yes, describe them.

(X) • Are there alarms for the computer and server areas for such things as unauthorized intrusion, loss of electric power, loss of environmental control, fire, and flooding or water intrusion? If yes, specify the types of alarms, how they are monitored, and the response procedure.

(X) (i) HVAC System (Air Handlers, Heating Plants, Cooling Towers, Chillers)

(X) Primary HVAC System

(X) • Can critical functions and activities dependent on environmental conditions continue without the HVAC system? If yes, specify which functions and for how long they can continue under various external weather conditions.

(X) • Is the HVAC system that supplies the areas of the asset/facility where critical functions dependent on environmental conditions are carried out separate from or separable from the general asset/facility-wide HVAC system?

(X) Supporting Infrastructures

(X) • Does the HVAC system (or critical portion thereof) depend on the primary electric power supply and distribution system to supply electric power? Specify under what conditions and for how long.

(X) • Besides or in addition to electric power, what fuel or fuels does the HVAC system (or critical portion thereof) depend.

(X) • If the HVAC system (or critical portion thereof) depends on natural gas, are there provisions for alternative fuels during a natural gas outage? Specify the fuel and how long the HVAC system can operate on it.

(X) • If the HVAC system (or critical portion thereof) depends on petroleum fuels for adequate operation, specify the type of fuel and how long the HVAC system can operate on the fuel available on site.

(X) • If the HVAC system (or critical portion thereof) depends on petroleum fuels, are arrangements and contracts in place for resupply and management of the fuel?

(X) • Does the HVAC system (or critical portion thereof) depend on water? If it does, specify if the water need is continuous or for make-up purposes only and the quantities/rates involved.

(X) • If the HVAC system (or critical portion thereof) depends on water, is a backup supply in place such as well and pump, storage tank, or tank trucks? Specify how long the HVAC can operate on the backup water supply system.

(X) Backup HVAC Systems

(X) • Is there a separate backup to the HVAC system? If yes, describe the system and the energy and water supply systems it requires.

(X) • Are there contingency procedures in place to continue with the critical functions and activities that take place at the asset/facility during an HVAC outage? If yes, briefly describe them.

(X) • How long can the critical functions and activities at the asset/facility continue using the backup HVAC system or under the contingency procedures?

(X) (j) Fire Suppression and Fire Fighting System

(X) Alarms

(X) • Does the entire asset/facility (or at least most of it) have a fire and/or smoke detection and alarm system? If yes, specify the type of system, how it is monitored, and the response procedure.

(X) Fire Suppression

(X) • Does the entire asset/facility (or at least most of it) have a fire suppression system such as an overhead sprinkler system? If yes, specify the medium (usually water) and whether it is of the flooded-pipe or pre-armed type.

(X) • Does the water supply for the fire suppression system come from city water mains or an on-site system, such as wells, rivers, or reservoir?

(X) • If the water supply for the fire suppression system comes from city water mains, specify whether there are separate city fire mains and if the pipe from the main to the asset/facility is separate from the domestic water supply.

(X) • If the water supply for the fire suppression system comes from an on-site system, specify the source, indicate the adequacy of the supply's capacity, and indicate if it is gravity feed or requires active pumps (generally electric).

(X) Fire Fighting

(X) • Does the asset/facility have its own fire-fighting department? If yes, describe it in terms of adequacy to protect the asset/facility.

(X) • Are city or community fire-fighting services available to the facility? If yes, indicate the type of service and the estimated response time.

(X) • Does the water supply for the fire-fighting hydrants come from city water mains? If yes, specify the number of hydrants and indicate their coverage and accessibility.

(X) • If the water supply for the fire fighting hydrants comes from an on-site system (such as wells, rivers, or reservoir), specify the source, indicate the adequacy of the supply's capacity, and indicate if it is gravity feed or requires active pumps (generally electric). Also, specify the number of hydrants and indicate their coverage and accessibility.

(X) Other Systems

(X) • Is there special fire suppression equipment, such as Halon, Inergen, inert gases, or carbon dioxide in certain areas such as computer or telecommunications areas? If yes, indicate the types and adequacies of these special systems.

(X) (k) SCADA System

(X) Type of System

(X) • Does the asset/facility make use of a substantial SCADA system (i.e., one that covers a large area or a large number of components and functions)? If yes, indicate what functions are monitored and/or controlled, the type of system, and the extent of the system.

(X) • Is the SCADA system independent of the asset's/facility's primary electric power supply and distribution system?

(X) • Is the SCADA system independent of the asset's/facility's telephone system?

(X) • Is the SCADA system independent of the asset's/facility's microwave or radio communications system?

(X) • Is the SCADA system independent of the asset's/facility's computers and servers?

(X) Control Centers

(X) • Where is the primary control center for the SCADA system located?

(X) • Is there a backup control center? If yes, where is it located? Is it sufficiently remote from the primary control center to avoid common causes of failure such as fires, explosions, or other large threats?

(X) • Are there backups to the SCADA computers and servers at the backup control center or at some other location? If yes, indicate the location of the backup computers and servers, whether they are completely redundant or cover only the most critical functions, and whether they are active “hot” standbys or have to be activated and initialized when needed.

(X) Note: *The following sets of questions on of electric power sources and communications pathways apply to the control centers as well as the other components of the SCADA system.*

(X) Electric Power Sources

(X) • Are there multiple sources of electric supply (such as multiple independent commercial feeds, backup generators, UPSs) explicitly for the SCADA system? If yes, indicate the types.

(X) • If there is a special UPS, does it support all the functions of the SCADA system in terms of capacity? Specify for how long it can operate on battery power.

(X) • If there is a special backup generator system, does it support all the functions of the SCADA system in terms of capacity?

(X) • What is the fuel or fuels used by the special SCADA backup generator system? If stored on site, specify the quantity stored and how long it will last.

(X) • If the SCADA backup generator fuel is stored on site, are arrangements and contracts in place for resupply and management of the fuel?

(X) Communications Pathways

(X) • Are there dedicated multiple independent telephone systems or dedicated switches and cables supporting the SCADA system? If yes, specify whether copper-wire or fiber-optic based.

(X) • If there are dedicated multiple independent telephone systems or dedicated switches and cables supporting the SCADA system, is each one individually adequate to support the entire system? Specify any limitations.

(X) • Are the redundant telephone systems or switches and cables physically separated and isolated to avoid common causes of failure? If not, indicate any potential points of common failure.

(X) • Are the dedicated SCADA telephone switches and data-transfer switches located in a limited access or secured area away from potential damage due to weather or water leaks? If so, specify type of protection.

(X) • Are there dedicated multiple or redundant radio communications systems in place to support the SCADA system? If yes, indicate the types.

(X) • If there are multiple radio communications systems, is each one individually adequate to support the entire SCADA system? If not, specify any limitations.

(X) • Are there provisions within the asset's/facility's primary electric power supply and distribution system to supply power for the special SCADA radio communications systems? If yes, specify under what conditions and for how long.

(X) • Do the special SCADA radio communications systems have their own backup electric power supply? If yes, specify the type and how long it can operate.

(X) • Are the components of the special SCADA radio communications system located outside of buildings (such as antennae, on-site towers) protected from vandalism or accidental damage by fences or barriers? If protected, specify the types of protection and level of security provided.

(X) Remote Components

(X) • Are there remote components to the special SCADA radio communications system (such as relay towers)? If yes, identify the components and there locations.

(X) • Are there backup sources of electric power for these remote components? If yes, indicate the type of backup, the fuels used, and the expected length of operations.

(X) • Are there environmental controls required for the remote components of the special SCADA radio communications system (such as heating, cooling)? If yes, describe them.

(X) • Are there backup environmental controls for these remote components? If yes, indicate the type of backup, the fuels used, and the expected length of operations.

(X) • Is physical security provided for the remote components of the special SCADA radio communications system? If yes, specify the types of security and the level of protection provided.

(X) • Are there alarms at the remote components of the special SCADA radio communications system for such things as intrusion, loss of electric power, loss of environmental control, and fuel reserves? If yes, specify the types of alarms, how they are monitored, and to the response procedure.

(X) Dedicated SCADA Computers and Servers

(X) • Are there provisions within the asset's/facility's primary electric power supply and distribution system to supply power for the special dedicated SCADA computers and servers? If yes, specify under what conditions and for how long.

(X) • Do the special dedicated SCADA computers and servers have their own backup electric power supply, such as local UPSs? If yes, specify the types and how long they can operate.

(X) • Does the asset's/facility's central HVAC system provide environment control for the separate special SCADA computer and server areas?

(X) • How long can the separate dedicated SCADA computers and servers operate with a loss of all environmental control? Indicate the conditions that could affect the length of time.

(X) • Do the separate dedicated SCADA computer and server areas have their own independent environmental control system? If yes, specify the type.

(X) • Are there any backup environmental controls explicitly for the dedicated SCADA computer and server areas? If yes, indicate the type of backup and the expected maximum duration of operation.

(X) • Is there special physical security provided for the separate SCADA computer and server areas? If yes, specify the type of security and the level of protection provided.

(X) • Is there special fire suppression equipment in the separate dedicated SCADA computer and server areas such as Halon, Inergen, inert gases, or carbon dioxide? If yes, specify the type of system.

(X) • Are there special features or equipment in the separate SCADA computer and server areas to limit flooding or water intrusion? If yes, indicate the precautions taken.

(X) • Are there alarms for the separate SCADA computer and server areas for such things as unauthorized intrusion, loss of electric power, loss of environmental control, fire, and flooding or water intrusion? If yes, specify the types of alarms, how they are monitored, and the response procedure.

(X) (I) Physical Security System

(X) Electric Power Sources

(X) • Are the asset's/facility's monitoring and alarm systems normally dependent on the asset's/facility's primary electric power supply and distribution system (i.e., is the asset's/facility's primary electric power supply and distribution system the primary electric power source?)?

(X) • Are there multiple sources of electric power for the monitoring and alarm systems? This could consist of the asset's/facility's primary electric power supply and distribution system and its backup or redundant systems; or combinations of multiple independent commercial electric feeds, backup generators, UPSs, or batteries dedicated to support the monitoring and alarm systems? Specify what electric power sources are in place.

(X) • If there is a special UPS, can it support all the functions of the monitoring and alarm systems in terms of capacity? Specify for how long it can operate on battery power.

(X) • If there is a special generator system, can it support all the functions of monitoring and alarm systems in terms of capacity? Also indicate the type of fuel or fuels used.

(X) • If the fuel for the special security generator system is a petroleum fuel, indicate the quantity stored on site and how long it will last. Are arrangements and contracts in place for resupply and management of the fuel?

(X) Communications Pathways

(X) • Are the asset's/facility's monitoring and alarm systems normally dependent upon the asset's/facility's telephone system?

(X) • Are there multiple independent telephone systems or dedicated switches and cables supporting the monitoring and alarm systems? This could consist of the asset's/facility's telephone system and its backup or redundant systems; or combinations of multiple independent telephone systems or dedicated communications lines. Specify the types of systems used and whether they are copper-wire or fiber optic-cable based.

(X) • Are the redundant telephone systems or switches and cables physically separated and isolated to avoid common causes of failure? If not, indicate any potential points of common failure.

(X) • Are the dedicated monitoring and alarm systems telephone switches and data-transfer switches located in a limited access or secured area away from potential damage due to weather or water leaks? If so, specify type of protection.

(X) • Are the asset’s/facility’s monitoring and alarm systems normally dependent upon the asset’s/facility’s microwave or radio communications system?

(X) • Are there multiple independent microwave or radio communications systems supporting the monitoring and alarm systems? This could consist of the asset’s/facility’s primary microwave or radio communications system and its backup or redundant systems; or combinations of multiple independent radios, antennae, and relay towers. Specify the type of radio systems used.

(X) • Are there multiple sources of electric power for the microwave or radio communications systems dedicated to support the monitoring and alarm systems? This could consist of the asset’s/facility’s electric power supply and distribution system and its backup or redundant systems; or combinations of multiple independent commercial electric feeds, backup generators, UPSs, or batteries dedicated to support the special microwave or radio communications systems. If yes, specify the types and how long they can operate.

(X) • Are the components of the special radio communications system dedicated to the monitoring and alarm systems that are located outside of buildings (such as antennae, on-site towers) protected from vandalism or accidental damage by fences or barriers? If protected, specify the types of protection and level of security they provide.

(X) • Are there remote components to the special radio communications system dedicated to the monitoring and alarm systems (such as relay towers)? If yes, identify the components and their locations.

(X) • Are there backup sources of electric power for the remote components? If used, indicate the type of backup, the fuels used, and the expected length of operations.

(X) • Are there environmental controls required for the remote components of the special monitoring and alarm radio communications system (such as heating, cooling)? If yes, describe them.

(X) • Are there backup environmental controls for the remote components? If yes, indicate the type of backup, the fuel or fuels used, and the expected length of operations.

(X) Computer Support

(X) • Are the asset’s/facility’s monitoring and alarm systems normally dependent upon the facility’s main computers and servers?

(X) • Are there multiple independent computers supporting the monitoring and alarm systems? This could consist of the asset's/facility's main computers and servers and their backup or redundant systems, or combinations of multiple independent computers. Specify the type of computers used.

(X) • Are there multiple sources of electric power for any computers dedicated to support the monitoring and alarm systems? This could consist of the asset's/facility's primary electric power supply and distribution system and its backup or redundant systems; or combinations of multiple independent commercial electric feeds, backup generators, or UPSs dedicated to support the monitoring and alarm systems. If yes, specify the type and how long they can operate.

(X) • Does the asset's/facility's central HVAC system provide environment control for the separate dedicated computers for the monitoring and alarm systems?

(X) • How long can the separate dedicated computers of the monitoring and alarm systems operate with a loss of all environmental control? Indicate the conditions that could affect the length of time.

(X) • Do the separate dedicated computers for the monitoring and alarm systems have their own independent environmental control system? If yes, specify the type.

(X) • Are there backup environmental controls explicitly for any dedicated computers of the monitoring and alarm systems? If yes, indicate the type of backup and the expected maximum duration of operation.

(X) (m) Financial System (Including Monetary Transactions)

(X) Electric Power Sources

(X) • Are the asset's/facility's financial systems and functions normally dependent on the asset's/facility's primary electric power supply and distribution system (i.e., is the facility's electric power supply and distribution system the primary electric power source?)?

(X) • Are there multiple sources of electric power for the financial systems and functions? This could consist of the facility's electric power supply and distribution system and its backup or redundant systems; or combinations of multiple independent commercial electric feeds, backup generators, or UPSs dedicated to support the financial systems and functions? Specify what electric power sources are in place.

(X) • If there is a special UPS, can it support all the financial systems and functions? Specify for how long it can operate on battery power.

(X) • If there is a special generator system, can it support all the financial systems and functions? Also indicate the type of fuel or fuels used.

(X) • Is the fuel for the special security generator system a petroleum fuel? Specify the quantity stored and how long it will last. Are arrangements and contracts in place for resupply and management of the fuel?

(X) Communications Pathways

(X) • Are the asset's/facility's financial systems and functions normally dependent upon the asset's/facility's telephone system?

(X) • Are there multiple independent telephone systems or dedicated switches and cables supporting the financial systems and functions? This could consist of the facility's telephone system and its backup or redundant systems; or combinations of multiple independent telephone systems or dedicated communications lines. Specify the types of systems used and whether they are copper-wire or fiber-optic cable based.

(X) • Are the redundant telephone systems or switches and cables physically separated and isolated to avoid common causes of failure? If not, indicate any potential points of common failure.

(X) • Are the dedicated telephone switches and data-transfer switches that support the financial systems and functions located in a limited access or secured area away from potential damage due to weather or water leaks? If so, specify the type of protection.

(X) Computer Support

(X) • Are the asset's/facility's financial systems and functions normally dependent upon the facility's main computers and servers?

(X) • Are there multiple independent computers supporting the financial systems and functions? This could consist of the facility's main computers and servers and their backup or redundant systems, or combinations of multiple independent computers. Specify the type of computers used.

(X) • Are there multiple sources of electric supply for any computers dedicated to support the financial systems and functions? This could consist of the asset's/facility's primary electric power supply and distribution system and its backup or redundant systems; or combinations of multiple independent commercial electric feeds, backup generators, or UPSs dedicated to support the financial systems and functions. If yes, specify the type and how long they can operate.

(X) • Does the asset's/facility's central HVAC system provide environment control for any separate dedicated computers that support the financial systems and functions?

(X) • How long can the separate dedicated computers that support the financial systems and functions operate with a loss of any environmental control? Indicate the conditions that could affect the length of time.

(X) • Do the separate dedicated computers that support the financial systems and functions have their own independent environmental control system? If so, specify the type.

(X) • Are there any backup environmental controls explicitly for the dedicated computers that support the financial systems and functions? If yes, indicate the type of backup and the expected maximum duration of operation.

LIST OF NOTATION (X)

(This page contains … .)

ANSER	Analytical Services, Inc.
CERT®	Carnegie Mellon University, Software Engineering Institute, Center of Internet Security Expertise, Coordination Center (CERT®/CC)
FBI	Federal Bureau of Investigation
HVAC	heating, ventilation, and air conditioning
InfraGuard	FBI-sponsored security group for information security and information technology professionals
NIPC	National Infrastructure Protection Center
OPSEC	operational security
P_E	probability of physical security system or system element effectiveness
PIN	personal identification number
RF	radio frequency
RFP	request for proposal
SCADA	supervisory control and data acquisition
TV	television
UPS	uninterruptible power supply